VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikačej techniky

# Siete pre distribúciu multicastov

# Networks for Multicast Distribution

2015

Bc. Martin Medera

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

# Zadání diplomové práce

Student: **Bc. Martin Medera**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T059 Mobilní technologie

Téma: Sítě pro distribuci multicastů
Networks for Multicast Distribution

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování sítí pro distribuci multicastů v laboratorním prostředí.

Osnova práce:
1. Popište problematiku multicastů a jejich šíření v síti.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň tři druhy sítí pro distribuci multicastů s využitím směrovačů Cisco a Huawei. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu směrovačů Cisco a Huawei v navržených sítích.

Seznam doporučené odborné literatury:

TEARE, Diane, et al. *CCNP Routing and Switching Foundation Learning Library: Foundation Learning for CCNP ROUTE, SWITCH, and TSHOOT (642-902, 642-813, 642-832)*. 1st ed. Indianapolis: Cisco Press, 2010. ISBN 978-1-58705-885-1.
Dokumentace k směrovačům Cisco a Huawei.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2014

Datum odevzdání: 07.05.2015

VYSOKÁ ŠKOLA BÁŇSKÁ TECHNICKÁ UNIVERZITA * OSTRAVA * Fakulta elektrotechniky a informatiky

doc. Ing. Miroslav Vozňák, Ph.D.
*vedoucí katedry*

prof. RNDr. Václav Snášel, CSc.
*děkan fakulty*

Prehlasujem, že som túto diplomovú prácu vypracoval samostatne. Uviedol som všetky literárné pramene a publikácie, z ktorých som čerpal.

V Ostrave 6. mája 2015 .....

Rád by som poďakoval Ing. Peterovi Machníkovi, Ph.D. za odbornú pomoc a konzultácie pri vytváraní tejto diplomovej práce.

## Abstrakt

Teoretická časť tejto práce popisuje problematiku multicastov a ich šírenia v sieti. V úvode vysvetľuje základné druhy komunikácie, z ktorých vyplýva výhodnosť použitia multicastu. V ďalšej časti je multicastová komunikácia vysvetlená detailnejšie.
V praktickej časti sú zostavené rôzne topológie za použitia jednotlivých protokolov pre distribúciu multicastu. V topológiach sú použité smerovače a prepínače od firiem Cisco a Huawei. Otestovaním navrhnutých topológii sa preukáže vzájomná kompatibilita týchto zariadení. Po úspešnom otestovaní v laboratórnom prostredí bude preukázané, že multicast môže byť šírený medzi týmito zariadeniami aj v reálnom svete.

**Kľúčové slová:** Cisco, Huawei, IGMP, MBGP, MLD, MSDP, Multicast, PIM

## Abstract

The theoretical part of this work describes multicasts and their distribution in the network. The introduction explains the basic types of communication which shows advantages of using multicast. The next part explaines multicast communication in more detail. In the practical part various topologies are assembled using different protocols for multicast distribution. These topologies are using routers and switches from Cisco and Huawei Companies. Testing of proposed topologies demonstrates cross-compatibility of these devices. After successful testing in a laboratory environment we will demonstrate that the multicast can be distributed between these devices in the real world.

**Keywords:** Cisco, Huawei, IGMP, MBGP, MLD, MSDP, Multicast, PIM

## Zoznam použitých skratiek a symbolov

| | | |
|---|---|---|
| ARP | Adress Resolution Protocol | Protokol rozlíšenia adries |
| AS | Autonomous System | Autonómny systém |
| BGP | Border Gateway Protocol | Hraničný smerovací protokol |
| BSR | Bootstrap Router | Bootstrap |
| DHCP | Dynamic Host Configuration Protocol | Protokol dynamickej konfigurácie hostov |
| DNS | Domain Name Server | Doménový server |
| DR | Designated Router | Poverený smerovač |
| DVMRP | Distance Vecstor Multicast Protocol | Vektorový multicastový protokol |
| GRE | Generic Routing Encapsulation | Generická enkapsulácia smerovania |
| IANA | Internet Assigned Numbers Authority | Internetová autorita pridelovania čísel |
| ICMP | Interet Control Message Protocol | Protokol riadiacich správ |
| IEEE | Institute of Electrical and Electronics Engineers | Inštitút Elektrických a elektronických inžinierov |
| IGMP | Internet Group Management Protocol | Internetový protokol správy skupín |
| IGP | Interior Gateway Protocol | Vnútorný smerovací protokol |
| IP | Internet Protocol | Internetový protokol |
| L2 | Layer 2 | Druhá vrstva ISO/OSI modelu |
| LAN | Local Area Network | Miestna sieť |
| LSA | Link State Advertisement | Správy protokolu OSPF |
| LSB | Less Significant Bit | Najmenej dôležitý bit |
| MAC | Media Access Control | Fyzická adresa |
| MBGP | Multiprotocol BGP | Multiprotocolový BGP |
| MLD | Multicast Listener Discovery | Objavenie poslucháča multicastu |

| | | |
|---|---|---|
| MOSPF | Multicast OSPF | Multicastový OSPF |
| MPEG | Motion Picture Experts Group | Skupina expertov pre pohiblivý obraz |
| MsgRcvd | Messages Recieved | Prijaté správy |
| MsgSend | Messages Sended | Odoslané správy |
| MSDP | Multicast Source Discovery Protocol | Protokol objavenia multicastoveho zdroja |
| OSI | Open Systems Interconnection | Referenčný model |
| OSPF | Open Shortest Path First | Smerovací protokol |
| PIM | Protocol Independent Multicast | Multicast nezávislý na protokole |
| PIM-DM | PIM-Dense Mode | PIM v hustom režime |
| PIM-SM | PIM-Sparse Mode | PIM v riedkom režime |
| RFC | Request For Comments | Žiadosť o komentáre |
| RP | Rendezvous Point | Bod stretnutia |
| RPF | Reverse Path Forwarding | Smerovanie spätnou cestou |
| RTP | Real-time Transport Protocol | Protokol komuniácie v realnom čase |
| SA | Source Active | Aktívny zdroj |
| TCP | Transssmission Control Protocol | Spojovo orientovaná služba |
| TTL | Time To Live | Doba životnosti |
| UDP | User Datagram Protocol | Nespojovo orientovaná služba |
| VLAN | Virtual Local Area Network | Virtualna lokálna sieť |
| VLC | Video LAN Connection | Multimediálny prehrávač |
| WAN | Wide Area Network | Rozlahlá sieť |

# Obsah

# Zoznam obrázkov

# 1 Úvod

Multicast je druh komunikácie jedného zdroja a skupiny príjemcov. Ako prirovnanie môže byť použité bežné rádio, kedy je jeden vysielač a množstvo prijímačov, ktoré dostávajú rovnaké dáta v rovnakom okamihu.

V praxi sa multicast používa napríklad pri internetovom rádiu, multiplayer hrách, video konferenciách a podobne. V prípade použitia unicastu by sa jednotlivé spojenia museli nadviazať pre každého príjemcu zvlášť. To by znamenalo značnú (a zbytočnú) záťaž pre sieť duplicitnými dátami.

Pomocou multicastu môžeme doručovať dáta súčasne skupine príjemcov efektívnym spôsobom, aby prechádzali sieťovým uzlom len jeden krát. Toto je zabezpečené tým, že sa dáta rozmnožujú len v mieste kde sa cesty k príjemcom rozdeľujú. Za týmto účelom vznikli rôzne multicastove smerovacie protokoly.

Cieľom tejto práce bude popísať problematiku multicastov a ich šírenia v sieti. Tieto informácie budú slúžiť na pochopenie výhodnosti použitia multicastu a ako samotný multicast funguje. V úvode práce sú vysvetlené základné druhy komunikácii v sieti (unicast, broadcast...). V nasledujúcej kapitole sú vysvetlené multicastové adresy spolu s odkazmi na presné určenia jednotlivých rozsahov vyčlenených pre potreby multicastov. Ďalej je popísaný princíp činnosti multicastu v LAN (Local Area Network) a vo WAN (Wide Area Network). V závere teoretickej časti sú rozobrané jednotlivé protokoly slúžiace na prihlasovanie hostov k multicastovým skupinám a protokoly slúžiace na distribúciu multicastu.

Ďalším cieľom práce bude realizovať rôzne druhy sietí za použitia smerovačov od firiem Cisco a Huawei a overiť na týchto sieťach ich kompatibilitu. Na otestovanie funkčnosti je nutné nejakým spôsobom generovať multicast. Počas testovania bude používaný VLC player a script v jazyku Python ako je popísané vo štvrtej kapitole. Ostatné kapitoly sa už venujú testovaniu jednotlivých multicastových protokolov, ktoré sú zariadeniami Cisco a Huawei podporované. Kapitoly pozostávajú z podkapitol venovaných nastaveniu aktívnych prvkov (presné konfigurácie sú obsiahnuté v prílohách) a overeniu funkčnosti daných konfigurácii. Počas overovania bude zdroj a príjemcovia multicastu premiestňovaný medzi aktívnymi prvkami tak, aby boli otestované všetky možné variácie zapojení.

Záver obsahuje zhodnotenia všetkých navrhnutých sietí pre distribúciu multicastov.

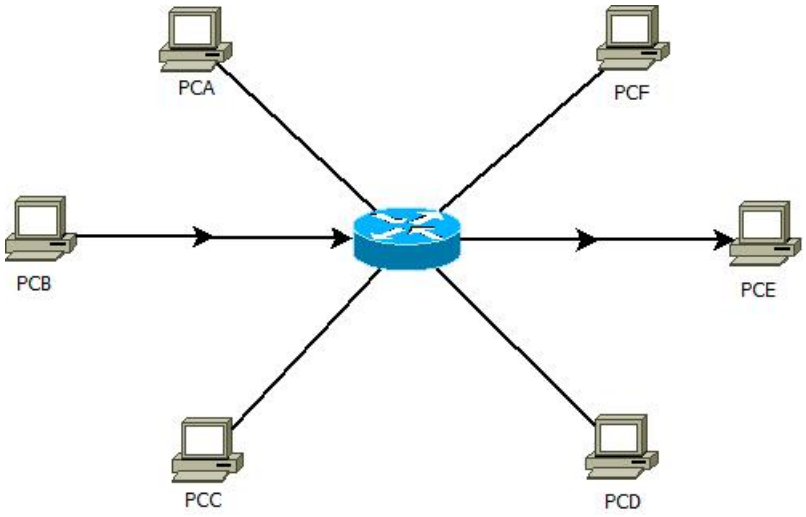
# 2 Druhy komunikácie v sieti

Ak chceme v počítačovej sieti poslať nejaké dáta je dôležité správne adresovanie správy, a s tým súvisí metóda vysielania. Je dôležité či chceme dáta odoslať len jednej stanici, skupine staníc alebo všetkým staniciam v rámci daného subnetu. Na základe týchto vlastností rozlišujeme unicast, anycast, broadcast, a multicast.

## 2.1 Unicast

Jedná sa o bežnú komunikáciu, kedy spolu komunikujú dve stanice. Unicast je vysielanie, kedy je paket zaslaný jednému cieľu (viď obr.2.1).

Tento spôsob nie je vhodný pre komunikácie kde je viac zdrojov a viac príjemcov, nakoľko by zdroj odosielal dáta toľko krát, koľko je odberateľov. Pre zdroj by to znamenalo plytvanie prenosovými prostriedkami rovnako ako pre sieť samotnú.

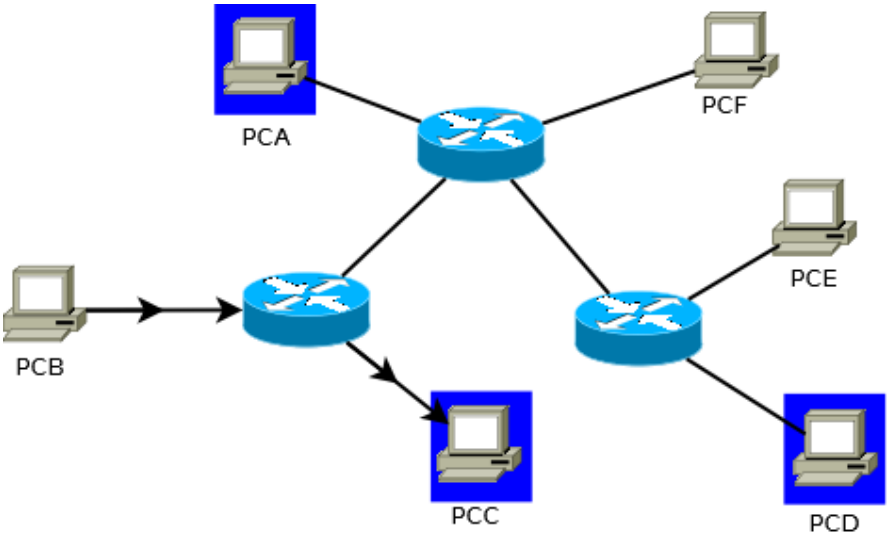



Obr. 2.1: Príklad komunikácie - Unicast

## 2.2 Anycast

Pri tomto druhu sú komunikujúcimi stranami zdroj a skupina príjemcov. Dáta sú smerované od zdroja do topologicky najbližšieho uzla skupiny potenciálnych príjemcov zjednotených rovnakou cieľovou adresou. Znamená to, že modro podfarbené stanice na obrázku 2.2 by v tomto prípade mali rovnakú IP adresu a sieť sa postará o doručenie topologicky najbližšiemu uzlu. Nevyžaduje špeciálne adresy ako multicast avšak nedoporučuje

sa na spojovo orientovené prenosy. Pracuje nad obyčajnými unicast adresami a komunikácia anycastu sa preto len ťažko rozoznáva od bežnej komunikácie. Obyčajne sa tento spôsob využíva pre koreňové DNS servery.

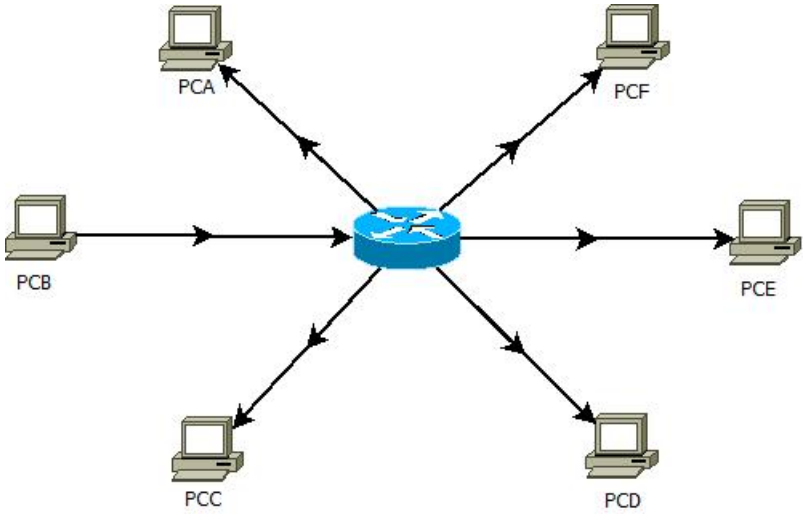



Obr. 2.2: Príklad komunikácie - Anycast

## 2.3 Broadcast

Tento druh komunikácie je vysielaním jedného všetkým (vid' obr.2.3). Paket je zachytený všetkými zariadeniami v sieti, presnejšie v danej broadcastovej doméne (subnete).

Používa sa obyčajne v sieťach LAN (Local Area Network). Využíva sa napríklad pre účely DHCP (Dynamic Host Configuration Protocol) či ARP(Address Resolution Protocol). Tvorí veľkú časť sieťovej komunikácie, pričom zaťažuje sieťové prvky a stanice, čo je dôvodom prečo vznikajú snahy o jeho minimalizáciu.

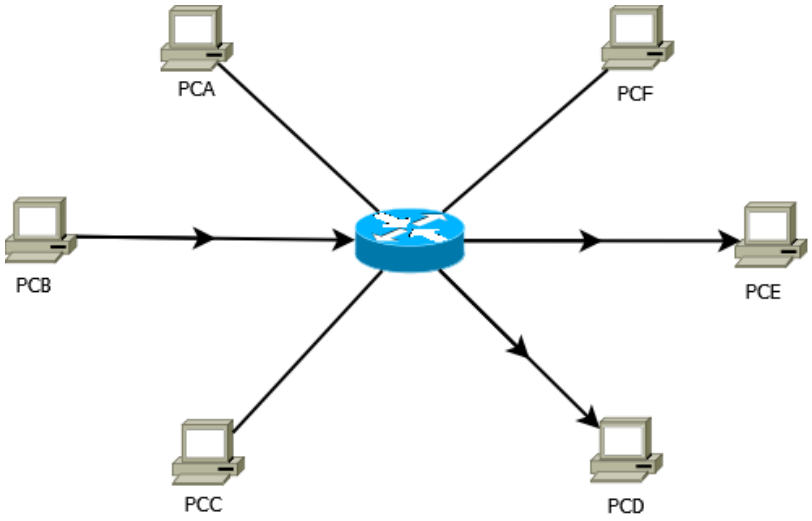



Obr. 2.3: Príklad komunikácie - Broadcast

## 2.4 Multicast

Pri tomto druhu komunikácie vysiela zdroj skupine príjemcov(viď obr.2.4). Multicast využíva efektívnu metódu doručovania, aby pakety putovali sieťou len jeden krát.

Vytvorí sa multicastová adresa a príjemcovia sa k tejto adrese zaregistrujú. Informácie o počte príjemcov nie sú pre zdroj dôležité, pretože kópie dát sa vytvárajú v smerovačoch, ktoré sú najbližšie k daným príjemcom.




Obr. 2.4: Príklad komunikácie - Multicast

# 3 Detajlnejší popis multicastu

Multicastové vysielanie je výhodné použiť všade tam, kde je potrebné doručiť informáciu skupine staníc beztoho, aby sme museli jednotlivé prúdy dát nesúce požadovanú informáciu od zdroja posielať ku všetkým jednotlivo.

Zdroj generuje len jeden tok dát a sieťové prvky ho zasielajú len do smerov, v ktorých ležia záujemcovia o daný dátový tok. Pre jednotlivých príjemcov sa pakety duplikujú až miestach, kde sa dátový tok rozdeľuje do viacerých vetví, v ktorých sa nachádzajú príjemcovia multicastovej skupiny. Spotrebované prenosové pásmo je teda výrazne menšie než keby boli toky generované pre príjemcov jednotlivo.

Distribúcia multicastových paketov sa odlišuje v LAN a WAN sieťach. V LAN je situácia jednoduchšia, pretože topológie neobsahujú slučky. Netreba v nich riešiť mechanizmy logického stromu.

## 3.1 Multicastové adresy

Vysielanie v súčasných technológiách LAN a v protokole IP pracuje s koncepciou otvorených skupín. Otvorenosť znamená, že do skupiny sa môže prihlásiť ktorákoľvek stanica a tiež to, že do skupiny môže vysielať aj stanica, ktorá sama nie je členom skupiny.

Jednotlivé stanice môžu byť súčasne členmi viacerých skupín. Prihlasovanie do skupín ovplyvňuje samotný prijímač každej skupiny. Zdroj dát nemôže zistiť identitu a počet príjemcov, ktorý v danom okamžiku prijímajú dáta.

### 3.1.1 MAC adresy

Na 2. vrstve OSI modelu sa v LAN obyčajne používajú na adresáciu MAC adresy. Prvé 3 bajty sú pridelené jednotlivým výrobcom, a tí potom prideľujú druhé 3 bajty jednoznačne jednotlivým kusom vyrábaných sieťových rozhraní.

Mimo jednoznačne pridelených adries môžu byť aj skupinové. Podľa IEEE sú skupinové adresy tie, ktoré majú prvý bit prvého bajtu MAC adresy vysielaného na médium nastavený na hodnotu 1 (v Ethernete je to LSB).

Pre IP protokol sa uvažujú ako skupinové MAC tie, ktoré začínajú trojicou 01-00-5E. Na 2. aj 3. vrstve môžu byť multicastove adresy len adresami cieľa. Zdrojová adresa musí byť vždy jednoznačná a identifikovať zdroj dát.

### 3.1.2 IPv4 a IPv6 adresy

V IPv4 protokole sú multicastové adresy v rozsahu triedy D, teda 224.0.0.0 až 239.255.255.255. Pre smerovacie protokoly a služobné protokoly na lokálnom segmente je vyhradený rozsah 224.0.0.0 - 224.0.0.255. Pre univerzálne protokoly využívajúce multicasting prideľuje organizácia IANA adresy z rozsahu 224.0.1.0 - 238.255.255.255 (detailný rozpis adries je dostupný online na stránkach IANA [2]).

Adresy, ktoré sa začínajú na trojicu bajtov 233.A.B môžu využívať správcovia autonómnych systémov bez prideľovacích procedúr, pričom číslo autonómneho systému kódujú do dvojice bajtov s hodnotami A a B (GLOP adresy).

Privátne skupinové adresy sú platné len v určitej oblasti, ktorú nesmú opustiť v rozsahu 239.0.0.0 - 239.255.255.255.

V IPv6 vyzerá obecná štruktúra multicastovej adresy nasledovne:

- FF00:/8 prefix multicastovej adresy
- Príznaky
- Identifikátor obsahu
- Identifikátor skupiny

Dosah vymedzuje oblasť v rámci ktorej sa môžu príjemcovia danej skupiny rozprestierať. V IPv6 sa skupiny rozdeľujú na známe (well-known) a dočasné (transient). Rozoznávame ich podľa príznakových bitov.

Identifikátory pre permanentné skupiny sú prideľované organizáciou IANA plošne a nie sú obmedzené dosahom. Naproti tomu identifikátory transientných skupín sú vždy unikátne len v rámci svojho dosahu.

### 3.1.3 Mapovanie IP na MAC

V lokálnych sieťach musíme riešiť mechanizmus na mapovanie IP adries na MAC adresy aj pri multicastovych adresách podobne ako to pre unicastové adresy rieši protokol ARP. Zabezpečenie mapovania je nutné, aby sa IP paket so skupinovou adresou mohol vložiť do rámca a určiť správnu cieľovú MAC adresu.

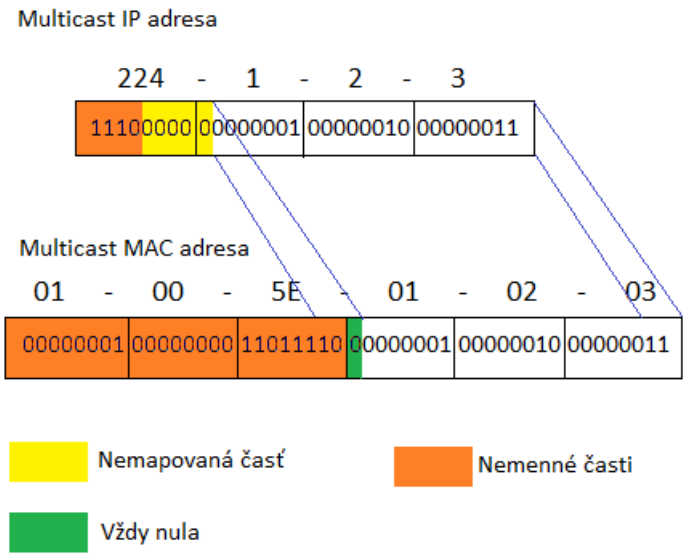
Multicastové MAC adresy, ktoré pripadajú multicastovým IPv4 adresám, majú výhradnú polovicu rozsahu adries začínajúcu 0x01:00:5E. Kvôli použitiu polovice spomínaného rozsahu je v najvyššom bite štvrtého bajtu MAC adresy vždy nula. Z toho vyplýva,

že k mapovaniu ostáva 23bitov. IPv4 má dĺžku 32bitov. No nakoľko všetky multicastove IP patria do skupiny D, začínajú vždy bitmi 1110, ktoré tým pádom nemusíme mapovať. Ostáva nám teda 28bitov, ktoré musíme namapovať do 23 bitov.

Mapovanie prebieha tak, že sa posledných 23bitov multicastovej IPv4 skopíruje do posledných 23bitov MAC adresy a posledných 5 najvyšších bitov IP adresy sa nemapuje. To znamená, že vždy 32 multicastových skupín sa mapuje na rovnakú MAC adresu (viď obr.3.1).

Nejednoznačné mapovanie, kedy spolu s vyžiadanou skupinou prijíma aj rámce 31 ďalších skupín riešia ovládače protokolu IP, ktoré nevyžiadané pakety filtrujú. Preto je vhodné adresy skupín voliť tak, aby nedochádzalo k prekrývaniu.

Multicastové adresy v IPv6 sa mapujú jednoduchšie. Majú stanovený 2 bajtový prefix multicastových MAC adries a najnižšie 4 bajty IPv6 adresy sa mapujú do najnižších 4 bajtov MAC adresy [1].




Obr. 3.1: Mapovanie IPv4 adresy na MAC adresu

## 3.2 Multicast v LAN

Multicastové vysielanie v lokálnej sieti neobsahuje slučky a je teda pomerne jednoduché. Výnimku tvorí len kruhová topológia, tu však rámec odstráni stanica ,ktorá ho po

obehnutí kruhu opätovne dostala. Ak sú stanice pripojené k zdieľanému médiu, počujú rámec vyslaný pre skupinu všetky stanice. Je teda v réžii staníc či rámec príjmu alebo nie.

O niečo zložitejšia situácia nastáva v sieti obsahujúcej prepínače. Vďaka protokolu Spanning Tree nevznikajú slučky ani tu. To znamená, že multicastové rámce môže bez rizika kopírovať na všetky porty okrem prichádzajúceho rovnako ako pri broadcaste. Takýmto spôsobom sa k multicastom stavajú lacnejšie prepínače. U drahších prepínačov sa zohľadňuje fakt, že na rozdiel od broadcastu nie je nutné multicastové pakety kopírovať na všetky porty, ale len do vetví, v ktorých sú príjemcovia danej multicastovej skupiny. To sa môžu dozvedieť nahliadaním do protokolu IGMP (spomínaný v nasledujúcej kapitole), alebo od špeciálneho protokolu zavedeného medzi smerovač a prepínač. Týmto protokolom predáva smerovač informácie prepínaču, ktoré MAC adresy majú záujem o prijímanie dát z multicastovej skupiny s adresou mapovanou na určitú MAC adresu.

## 3.3 Multicast vo WAN

WAN obsahujú slučky, preto na distribúciu multicastového paketu vyžadujú konštrukciu distribučného stromu, ktorého vetvy budú pokrývať všetky časti WAN v ktorých sa nachádzajú záujemcovia o prijímanie danej multicastovej skupiny. Za koreň je určený buď smerovač, v ktorom je umiestnený zdroj multicastov alebo smerovač, do ktorého tunelovým spojením posielajú zdroje svoje pakety. V prípade, že nechceme pre skupinu vytvárať toľko stromov koľko je zdrojov multicastu.

Smerovač na základe znalosti svojej pozície v distribučnom strome rozlíši či rozhranie z ktorého multicastové pakety prichádzajú vedie ku koreňu distribučného stromu a určí rozhrania, za ktorými sú aktívni príjemci danej multicastovej skupiny. Na základe informácie o pozícii smerovača v strome pre danú skupinu si smerovače na šírenie multicastov vytvárajú zvláštnu formu smerovacej tabuľky, v ktorej sú obsiahnuté informácie o rozhraniach vedúcich k zdroju a do vetví s príjemcami.

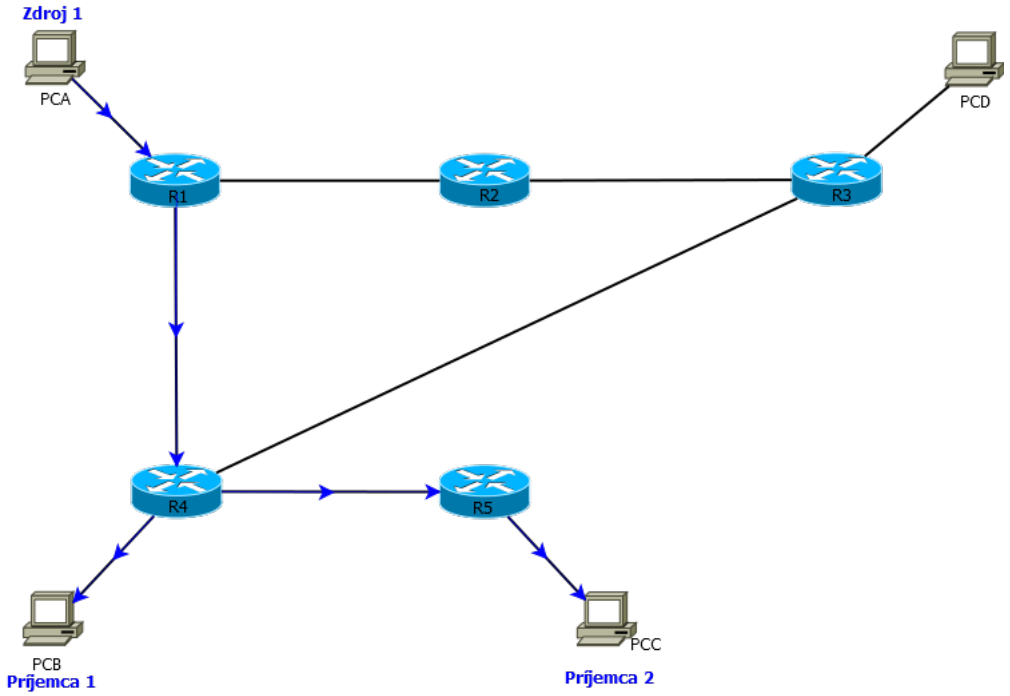
### 3.3.1 Distribučné stromy

Distribučný strom je podgrafom grafu topológie, ktorý neobsahuje slučky a zahŕňa všetky siete, na ktorých sú príjemcovia multicastovej skupiny. Kvôli prihlasovaniu nových a ohlasovaniu existujúcich príjemcov sa do stromu musia pripájať nove vetvy a odstraňovať neaktuálne (ang. grafting a prunning ).

Rozoznávame niekoľko spôsobov ako distribučný strom konštruovať. Na základe toho kde je umiestnený koreň stromu rozdeľujeme stromy na zdrojové (Source Tree často aj Shortest-Paths Tree) a zdieľané (Shared Tree). Priebeh komunikácie v strome býva jednosmerný (od koreňa k listom) alebo obojsmerný, kde sa komunikácia šíri vše smerovo od zdroja k niektorému uzlu stromu [1].

#### 3.3.1.1 Zdrojový strom

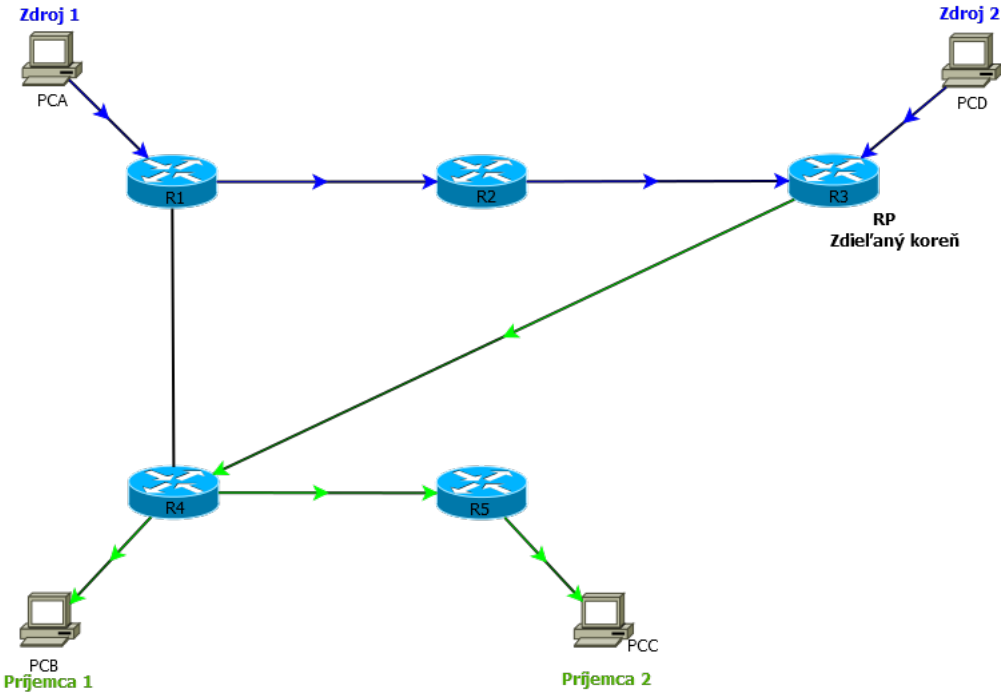
Zdrojový strom je strom najkratších ciest zo zdroja do všetkých sietí s príjemcami skupiny. Toto riešenie je optimálne avšak málo škálovateľné. Komunikácia má síce najmenšie oneskorenie, ale pre každý zdroj vysielania do každej multicastovej skupiny musí existovať samostatný strom (používa sa označenie <S,G>, S - zdrojová adresa, G - adresa multicastovej skupiny). Ukážka na obrázku 3.2 zobrazuje zdrojový distribučný strom. Na obrázku je naznačený šípkami.




Obr. 3.2: Zdrojový distribučný strom

#### 3.3.1.2 Zdieľaný strom

Zdieľaný strom je spoločný pre všetky zdroje v skupine. Za koreň sa volí vhodný smerovač (Rendezvous point - RP). Na RP zasielajú zdroje svoje dáta a on ich rozširuje smerom dole po distribučnom strome (používa sa značenie <*,G>, * - strom používa všetky zdroje prispievajúce do skupiny, G - skupina). Pre multicastovú skupinu postačuje jeden strom bez ohľadu na počet zdrojov. Kvôli dlhšej ceste paketov od zdroja k RP a následne k príjemcom vzniká väčšie oneskorenie. Ukážka na obrázku 3.3 zobrazuje zdieľaný distribučný stom. Na obrázku je naznačený šípkami.




Obr. 3.3: Zdieľany distribučný strom

## 3.4 Prihlasovanie do skupín

V prípade, že sa stanica na LAN chce prihlásiť k odberu toku určitej multicastovej skupiny, použije k tomu v IPv4 protokol IGMP (Internet Group Membership Protocol) [22] a v IPv6 protokol MLD (Multicast Listener Discovery) [19]. Vďaka nim oznamujú lokálnemu smerovaču, že ma požiadať centrálne smerovače o rozšírenie distribučného stromu, aby pokryl i segment s príjemcom. Podobným spôsobom môžu stanice signalizo-

vať týmito protokolmi aj situáciu, že už nechcú tok od určitej skupiny odoberať. Lokálny smerovač ešte dotazom overí či na segmente nie je žiadna ďalšia stanica, ktorá má záujem o tok skupiny, V prípade, že nie tak zasielanie multicastu na lokálny segment ukončí a do WAN pošle žiadosť o prerezanie distribučného stromu. Z dôvodu, že prijímač môže byť nekorektne vypnutý bez informovania lokálneho smerovača, overuje smerovač periodickými dotazmi či stanice majú o príjem svojej skupiny aj naďalej záujem.

### 3.4.1 Protokol IGMPv1

Táto verzia pozostáva z dvoch správ. Prvou správou je Host Membership Query. Túto správu odosiela multicastovy smerovač na objavenie, ktoré skupiny hostov majú členov na jeho lokálnej sieti. Dotazy sú adresované na všetkých hostov skupiny a nesú v IP hodnotu TTL nastavenú na 1. Hostovia odpovedajú správou Host Membership Report [3] . Odpovede sú zasielané jedným hostom za celú skupinu, ktorá patrí na sieťové rozhranie, z ktorého bol dotaz obdržaní. Ak stanica prestane mať záujem o odoberanie multicastových tokov tak prestane odpovedať na dotazy smerovača.

### 3.4.2 Protokol IGMPv2

Táto verzia zachováva spätnú kompatibilitu s IGMPv1 pričom rozširuje funkčnosť IGMP. Prináša novú správu Leave Group pomocou ktorej sa stanice môže odhlásiť z multicastovej skupiny. Výhodou je zníženie oneskorenia odhlásenia. Nová je aj možnosť špecifického dotazovania priamo na záujemcov o jednu konkrétnu multicastovu skupinu v správe Membership Query (Group Specific Query) [4].

### 3.4.3 Protokol IGMPv3

Najnovšia verzia zachováva spätnú kompatibilitu s verziou 1 a verziou 2, pričom IGMP rozširuje o možnosť filtrovania požadovanej komunikácie na základe zdrojových adries. Tým je možné brániť sa pred nekorektne sa chovajúcimi stanicami, ktoré zahlcujú multicastovú skupinu. Pri žiadosti o komunikáciu multicastovej skupiny je potom možné jednoznačne zadať zoznam zdrojov, ktoré môžu správy šíriť alebo zadať zoznam zdrojov, od ktorých majú byť správy filtrované [5].

### 3.4.4 Protokol MLDv1

Protokol MLD je ekvivalentom IGMP. Hlavným rozdielom (okrem verzie IP) je, že MLD je integrálnou súčasťou ICMPv6 správ, zatiaľ čo v prípade IPv4 šlo o samostatný protokol.

Z toho vyplýva, že MLD správy vychádzajú zo správ ICMPv6 a preto je formát správy podobný [20]. MLD využíva tri druhy správ. Prvou je správa Multicast Listener Query. Pomocou tejto správy zisťuje smerovač členov skupiny v rámci sieťového segmentu. Ďalšou správou je Multicast Listener Report. Táto správa je odosielaná hostom pri pripojení do skupiny alebo ako odpoveď na Multicast Listener Query. Posledným typom správy je Multicast Listener Done. Tú odosiela v prípade, keď ako posledný opúšťa skupinu.

### 3.4.5 Protokol MLDv2

Tento protokol rozširuje predchádzajúcu verziu o možnosť filtrovať vysielacie zdroje. Využívajú sa k tomu príkazy INCLUDE a EXCLUDE [21]. Pomocou týchto pravidiel je možne vykonať všetky logické operácie ako je prienik či zjednotenie. INCLUDE definuje, od ktorých zdrojov chceme prijímať multicast a EXCLUDE naopak, ktoré zdroje budú odmietnuté.

### 3.4.6 IGMP Snooping

Jedná sa o optimalizačný mechanizmus pre L2 switche. V štandardnom prípade sa šíri multicast na switchoch ako broadcast. To znamená, že sú dáta preposielané na všetky porty okrem prichádzajúceho. Tento mechanizmus zabezpečuje detekciu správ join a leave a podľa toho sa učí, na ktorom porte sa nachádza router a kde klienti. Zostavuje si tabuľku podľa ktorej preposiela multicast len tam, kde je požadovaný. Rovnako odpovede klientov odosiela len na router a nie susedným klientom. Jedná sa teda o spôsob ako dynamicky konfigurovať porty pre príjem multicastu [22].

### 3.4.7 MLD Snooping

Rovnako ako pri IGMP snoopingu sa jedná o mechanizmus, ktorý zabraňuje switchom aby zaobchádzali s multicastom rovnako ako s broadcastom [19].

Prepínače, ktoré pripájajú koncové uzly najskôr odpočúvajú MLD komunikáciu a na základe takto získaných informácií rozhodujú, o ktoré multicastové skupiny má koncový uzol záujem.

## 3.5 Smerovanie multicastu

Hlavnou úlohou smerovania multicastov je nájsť cesty v sieti tak, aby mohla prevádzka efektívne dosiahnuť na každého člena jednotlivých skupín. Pomocou smerovacích protokolov hľadajú smerovače minimálny strom spojov pokrývajúci cestu od zdroja k aktuálnym záujemcom o prijímanie skupinového vysielania. Na rozdiel od klasického smerovania v unicaste ide o veľmi dynamický proces. Vyplýva to z faktu, že záujemcovia o príjem daného skupinového vysielania môžu vznikať a zanikať. Tento proces priebežných zmien musia smerovacie protokoly vhodne odrážať.

Smerovanie multicastu sa realizuje v dvoch režimoch:

- **Hustý režim (dense mode)** predpokladá, že príjemcovia konkrétnej multicastovej relácie sú takmer všade. Čiže, každý prijatý multicastový datagram sa posiela na všetky sieťové rozhrania okrem RPF (Reverse Path Forwarding) rozhrania, z ktorého datagram prišiel. V prípade, že niektorý smerovač nechce od svojho suseda dostávať určitú skupinu, musí mu ho o tom explicitne informovať. Medzi tieto protokoly patria napríklad DVMRP alebo PIM-DM.
- **Riedky režim (sparse mode)** predpokladá naopak, že príjemcov je minimálny počet a preto sám od seba prijaté multicastové datagramy nikam neposiela. Pre príjem multicastovej skupiny ho musí smerovač o to požiadať. Medzi tieto protokoly patri napríklad PIM-SM.

### 3.5.1 Protokol DVMRP

Protokol DVMRP (Distance Vector Multicast Routing Protocol) pracuje s vlastným smerovacím mechanizmom založeným na algoritme vektorov vzdialenosti[6]. Smerovače po prijatí paketu určeného pre skupinu odošlú tento paket na všetky rozhrania okrem toho, z ktorého prišiel. Tým sa má zaručiť dosažiteľnosť všetkých sietí i kde sa týmto spôsobom občas vytvorí niekoľko kópií paketu. Následne dostane smerovač informácie z oslovených sietí o tom či obsahujú alebo neobsahujú stanice z danej skupiny. Vďaka tomu sa nevytvára distribučný strom naraz ale postupne. Tento smerovací protokol spôsobuje

zaťažovanie siete častým záplavovým smerovaním preto sa často používa tunelovací mechanizmus. Dnes sa už príliš často nepoužíva a bol nahradený PIM-DM. Podrobný popis tohto protokolu nájdete v RFC 1075. Detailným popisom sa v práci nezaoberám, nakoľko spoločnosť Huawei nikde neuvádza podporu tohto protokolu a u spoločnosti Cisco je momentálne podpora iba čiastočná[7].

### 3.5.2 Protokol PIM-DM

PIM-DM (Protocol Independent Multicast - Dense Mode) funguje nezávisle na použitom smerovacom protokole a smeruje multicast na základe zdroja[16]. Jeho nasadenie je vhodné do silnej skupinovej prevádzky o malom počte zdrojov a veľkom počte príjemcov v skupinách. Taktiež sa používa v konštantnej skupinovej prevádzke fyzicky blízkych zdrojoch a cieľoch skupinového vysielania. Tento protokol počíta s rýchlou sieťou a dostatočne širokým pásmom. Funguje na podobnom princípe ako DVMRP. Všetky podsiete zaplavuje multicastovými datagramami, až kým nedostane správu o neprítomnosti žiadneho člena danej podskupiny v cieľovej podsieti. Potrebuje bežné smerovacie informácie no na rozdiel od DVMRP nedokáže inzerovať konvenčné cesty. Je postavený na tom, že smerovač sa postará o dobré znalosti topologie a výber najlepších ciest sieťou.

### 3.5.3 Protokol MOSPF

Tento protokol rozširuje OSPF (Open Shortest Path First) o podporu smerovania multicastov. LSA sú smerovačmi rozosielané tak, aby mali všetky smerovače rovnaké znalosti o členoch pre danú multicastovu reláciu. Stavové pakety obsahujú informácie o aktívnych skupinách na jednotlivých segmentoch. Každá dvojica zdroja a skupiny príjemcov má vlastný distribučný strom s koreňom pri zdroji. Protokol je založený na strome najkratších ciest, ktorý sa buduje naraz. Cesty sú vyberané podľa metriky.

Je vhodný pre relatívne malý počet aktívnych staníc nakoľko posiela datagramy len v prípade skutočnej potreby . Protokol je náročný z hľadiska záťaže smerovača, pretože každý smerovač si neustále udržuje informácie o všetkých existujúcich skupinách a prepočítava strom najkratších ciest pri každej zmene v členstve skupín.

### 3.5.4 Protokol PIM-SM

PIM-SM (Protocol Independent Multicast - Sparse Mode) vychádza z predstavy, že v sieti sa nachádza veľmi malý počet klientov, ktorí chcú prijímať multicast. Takže sparse mode

posiela prevádzku len smerovačom, ktoré si o príjem požiadali.

Používa jednosmerné zdielané stromy s koreňom v RP (Rendzevous Point) a môže vytvárať stromy najkratších ciest pre zdroje, vyžaduje na sieti RP. Zdroje posielajú multicast priamo pripojeným smerovačom (DR - Designated Router), DR (smerovač s najvyšším IP) ich zabalí ako unicast a pošle na RP. Ten ich posiela členom multicastovej skupiny. RP oznamuje zdroje a vytvára cestu od zdroja k členom skupiny a až potom posiela multicastové datagramy.

Jeho použitie je vhodné tam, kde ide o veľký počet skupín ale malý počet príjemcov v rámci skupiny alebo pri prítomnosti diaľkových spojov.

#### 3.5.4.1 PIM SM s použitím BSR (automatická voľba RP)

Jedná sa o spôsob ako automaticky informovať smerovače na sieti o RP pre rôzne multicastové skupiny. Nieje tým pádom nutné manuálne konfigurovať všetky smerovače. V prípade výpadku sa potom dokáže obstarať nový RP automaticky.

Pôvodne existoval Cisco Proprietárny protokol s názvom Auto RP[17], ale časom vznikol v podstate rovnaký protokol s názvom BSR (Bootstrap router)[8], ktorý zabezpečuje rovnaký účel.

Narozdiel od Auto RP nepoužíva BSR žiadne dense-mode skupiny. BSR postupne zbiera všetkých kandidátov na RP a vytvára zoznam, ktorý sa distribuuje pomocou PIM správ. Pracuje v dvoch fázach:

- **Fáza 1.** BSR Discovery. Každý smerovač nastavený ako BSR naplavuje bootstrap správy a počúva ostatných BSR kandidátov. BSR ktorý počuje iný BSR s vyššou prioritou než má predáva svoju rolu jemu. Nakoniec je len jeden BSR a každý smerovač v doméne mu predáva informácie o kandidátoch na RP.

- **Fáza 2.** RP Discovery. Každý RP unicastom posiela svoju adresu BSR smerovaču. BSR sa takto naučí všetky RP a opakovane naplavuje nové informácie skrz doménu.

#### 3.5.4.2 PIM SM Anycast RP

Anycast RP[18] je riešenie, ktoré zabezpečuje ochranu proti výpadku a rozkladanie záťaže (load balancing) medzi ľubovolný počet aktívnych RP v doméne. Všetky RP v multicastovej doméne zdieľajú rovnakú IP adresu. Správy protokolu PIM (join/prune aj registrácia zdroja) sú potom odosielané najbližšiemu RP na základe unicastovej smerovacej tabuľky.

Toto riešenie je čisto vnútro doménová záležitosť a nedá sa aplikovať medzi doménami. Aj keď je postavené na využití protokolu MSDP (Multicast Source Discovery protocol), ktorý je primárne používaný práve na účel prepájania domén.

MSDP je povolené medzi RP a beží po TCP spojení (port 639). Tento protokol dovoľuje rendevouz pointom vymieňanie informácií o multicastových zdrojoch.

### 3.5.5 Protokol MBGP

Multiprotocol Border Gateway Protocol pridáva protokolu BGP schopnosť smerovať multicast naprieč internetom a spájať multicastové topologie medzi autonomnymi systémami. MBGP je teda rozšírenie, ktoré nesie multicastové cesty.

Základná myšlienka za MBGP (keď sa používa v súvislosti s multicastom prisudzuje sa písmenu M význam multicast namiesto multiprotocol) je definovanie dvoch nových multiprotocol BGP atribútov, ktoré sú použité na vymieňanie informácií o dosažiteľnosti pre rozdielne rodiny adries. Tieto rodiny adries (Address Family) sa prenášajú vnútri BGP update správ.

Protokol BGP teda prenáša dve skupiny ciest, jedny pre klasický unicast a jedny pre multicast. Cesty asociované k multicastu sú následne používané protokolom PIM na zostavenie distribučného stromu [23].

### 3.5.6 Protokol MSDP

Tento protokol umožňuje prepojenie multicastových smerovacích protokolov v rôznych doménach (autonómnych systémoch). V každej doméne môže byť vlastný RP (Rendevouz Point) nezávisle na ostatných doménach. Smerovače prepojené MSDP si vymieňajú informácie o zdrojoch multicastu. Tieto smerovače (peery) udržujú medzi sebou TCP spojenie, ktorým vytvárajú v podstate virtuálnu topológiu, nad ktorou sa vytvára distribučný strom.

V prípade, keď sa RP dozvie o novom zdroji multicastu zabalí (encapsuluje) prvý paket do správy SA (Source-Active) a pošle ho spomínaným TCP spojením ostatným MSDP peerom. Každý z nich tento paket rozbalí a v prípade, že vo svojej doméne má odberateľa pre daný multicast, pošle ho svojím distribučným stromom. TCP spojenie medzi peermi je udržované periodickým zasielaním KeepAlive správ [26].

# 4 Vytváranie multicastového vysielania

Testovanie jednotlivých multicastových protokolov prebiehalo pomocou prenosu videa za využitia VLC playeru (dostupné z [9]) a scritpu napísaného v jazyku Python. Prostredníctvom týchto nástrojov bol vytvorený multicastový prenos. Pri použití VLC playeru sa objavil problém s hodnotou TTL v prenosovom reťazci, ktorá je defaultne nastavená na 1, aby pakety neopúšťali segment siete.

Dáta prenosu som následne odchytával pomocou programu Wireshark [13].

## 4.1 VLC player

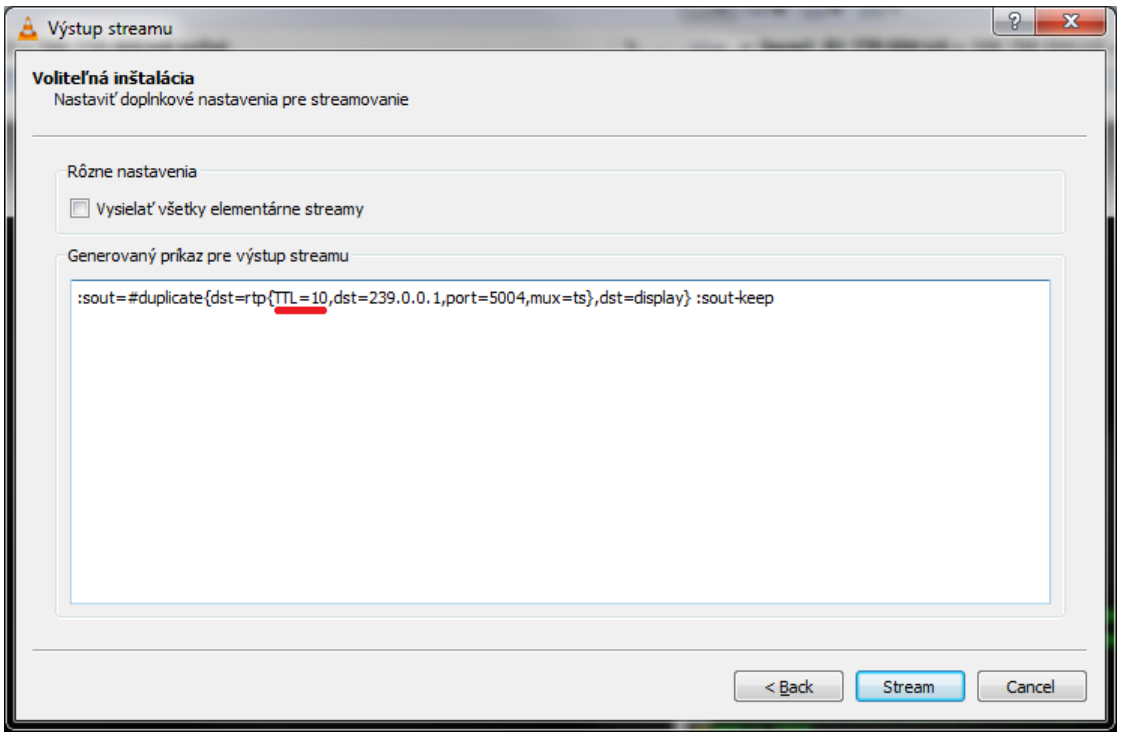
Na vysielanie som využíval video stiahnuté zo stránky Vimeo [10]. Podľa interných podmienok tohto serveru môžu byť videá, ktoré autor umožnil stiahnuť použité na školské účely (viď [11]).

Pre multicastové vysielanie je nutné správne nastaviť VLC player [12]. Postup nastavenia pre vysielaciu stranu je nasledovný:

1. V Medium menu vyberieme možnosť *Stream* (alebo stlačenie skratky Ctrl+s).
2. V dialógu Otvoriť médium klikneme na položku pridať a vyberieme video, ktoré chceme prenášať.
3. V spodnej časti okna klikneme na tlačítko *Stream* (prípadne na šípku vedľa tlačítka Prehrať a vyberieme možnosť Stream).
4. Objaví sa okno Výstup streamu, kde je uvedený zdroj videa (cesta k súboru). V tomto okne klikneme na tlačítko *Ďalej*
5. Pokiaľ chceme vidieť prenášané video aj priamo na zdrojovej stanici zaklikneme položku *Zobraziť lokálne*. V rozbaľovacom menu *súbor* vyberieme možnosť *RTP /MPEG Transport Stream* a následne klikneme na tlačítko *Pridať*
6. Zobrazí sa okno Výstup Streamu. Tu je nutné zadať adresu multicastu (ja som obyčajne používal adresu 239.0.0.1) a vybrať port (prednastavená hodnota 5004). Potom klikneme na tlačítko *Ďalej*
7. Zobrazí sa okno, kde môžeme nastaviť prekódovanie videa. Ja som túto funkcionalitu nevyužíval, preto som odklikol možnosť *Aktivovať prekódovanie*, ktoré je defaultne zapnuté.

8. Posledné okno zobrazuje vygenerovaný príkaz pre výstup streamu (viď obr.4.1). Tu je nutné doplniť vhodnú hodnotu TTL (upozorňujem, že umiestnenie hodnoty má vplyv na to či prenos bude fungovať).

9. Potom stačí kliknúť na tlačítko *Stream*.




Obr. 4.1: Výstup streamu

Nastavenie na strane príjemcu multicastu:

1. V menu Medium klikneme na možnosť *Otvoriť stream v sieti* (alebo stlačíme klávesovú skratku ctrl + n)

2. Zobrazí sa okno Otvoriť médium. Do textového políčka zadáme podľa uvedených príkladov adresu a port multicastu (v mojom prípade to bolo rtp://@239.0.0.1:5004)

3. Nakoniec klikneme na tlačítko *Prehrať*.

## 4.2 Script v jazyku Python

Script, ktorý som využíval na overenie funkcionality multicastu je vzorový príklad priamo zo stránok Pythonu [14].

Jeho používanie je jednoduché a na základné overenie je dostačujúci. Pri testovaní som pracoval pod operačným systémom Linux Xubuntu. Script je nutné nakopírovať do počítača potom v terminále vstúpiť do zložky kde je umiestnený. Samotný script sa spúšťa nasledovne:

- Na vysielacej strane:
  - **pre IPv4** *sudo python mcast.py -s*
  - **pre IPv6** *sudo python mcast.py -s -6*
- Na strane príjmu:
  - **pre IPv4** *sudo python mcast.py*
  - **pre IPv6** *sudo python mcast.py -6*

Ukážka zdrojového kódu je v prílohe A (Prílohy). Script obsahuje údaje o multicastovej adrese, porte a hodnote TTL, ktoré sú v stave bez modifikovania nastavené nasledovne:

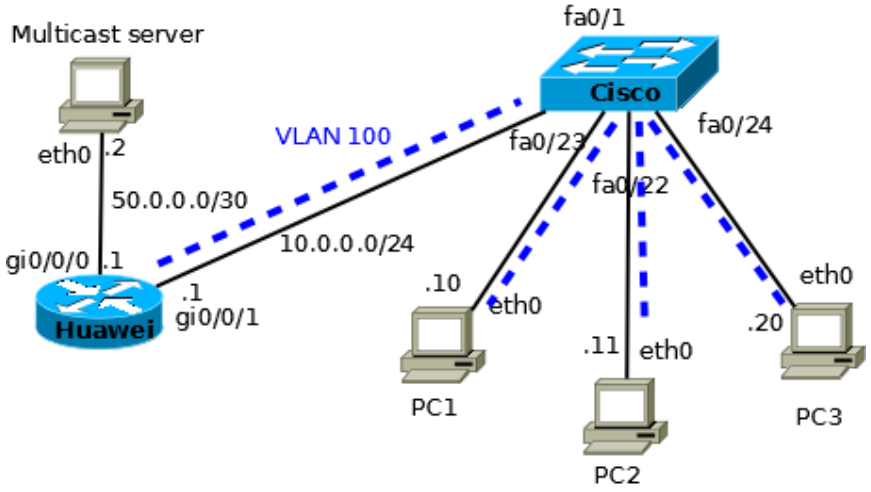
- $MYPORT = 8123$ ...*Port*
- $MYGROUP\_4 =' 225.0.0.250'$ ...*Multicastová adresa IPv4*
- $MYGROUP\_6 =' ff15:7079:7468:6f6e:6465:6d6f:6d63:6173'$...*Multicastová adresa IPv6*
- $MYTTL = 1$ ...*Hodnota TTL*

# 5 Konfigurácia IGMP Snooping

Táto konfigurácia je situovaná na prepínači a nahliada do datagramov vyššej vrstvy. Pri tejto konfigurácii som testoval ako dokáže pracovať prepínač firmy Huawei s paketmi, ktoré prichádzajú od smerovača firmy Cisco a naopak. Ďalej som testoval, ako reagujú na pakety, ktoré prichádzajú v hustom režime (na smerovači beží PIM-DM) a ako na pakety v riedkom režime (na smerovači beží PIM-SM). Pri testovaní som používal switch Huawei Quadway S5328C-PWR-EI a Cisco Catalyst 2960.

## 5.1 Nastavenia prepínačov

Sieť bola zapojená podla topológie na obrázku 7.1. Pomenovania aktívnych prvkov v tejto schéme sú len ilustračné, pretože som testoval obe varianty. To znamená, že okrem zobrazeného stavu som overoval kompatibilitu aj vo vzťahu Cisco smerovač a Huawei prepínač. Pričom ostatné zobrazené zostávalo rovnaké.




Obr. 5.1: Topológia siete pre IGMP Snooping

Konfigurácia na prepínači Cisco vyzerá následovne:

- Aktivácia IGMP Snooping (v základnom stave je povolený)
  - *switch(config)# ip igmp snooping*
- Vstup do konfiguračného moodu pre VLAN, v ktorej chceme IGMP Snooping využívať

  - *switch(config)# vlan <vlan-id>*

- Povolenie IGMP Snooping pre danú VLAN

  - *switch(config-vlan)# ip igmp snooping*

Konfigurácia na prepínači Huawei:

- Aktivácia IGMP Snoopingu

  - *[switch]igmp-snooping enable*

- Vstup do konfiguračného moodu pre VLAN, v ktorej chceme IGMP Snooping využívať

  - *[switch] vlan <vlan-id>*

- Povolenie IGMP Snoopingu pre danú VLAN

  - *[switch-vlan]igmp-snooping enable*

Skrátená konfigurácia prepínača Huawei je v prílohe E.1 a prepínača Cisco prílohe E.2 (Prílohy). Konfiguráciám smerovačov sa v tejto kapitole nevenujem, pretože sú rozoberané v neskorších kapitolách. Preto ich z hľadiska popisu IGMP snoopingu budeme chápať viacmenej ako zdroj multicastu.

## 5.2 Overenie funkčnosti konfigurácie

IGMP snooping medzi zariadeniami Cisco a Huawei fungoval správne, o čom nasvedčujú nasledujúce výpisy. Informácie o nastavení samotného IGMP Snoopingu a o tom, že je aktivovaný vidíme na obrázkoch 5.3 a 5.2

```
[HUswitch]dis igmp-snooping vlan 100
  IGMP Snooping Information for VLAN 100
     IGMP Snooping is Enabled
     IGMP Version is Set to default 2
     IGMP Query Interval is Set to default 125
     IGMP Max Response Interval is Set to default 10
     IGMP Robustness is Set to default 2
     IGMP Last Member Query Interval is Set to default 1
     IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
     IGMP Filter Group-Policy is Set to default : Permit All
     IGMP Prompt Leave Disable
     IGMP Router Alert is Not Required
     IGMP Send Router Alert Enable
     IGMP Proxy Disable
     IGMP Report Suppress Disable
     IGMP Suppress Time is set to default 10 seconds
     IGMP Querier Disable
     IGMP Router Port Learning Enable
     IGMP SSM-Mapping Disable
     IGMP Limit Action Disable
     IGMP Suppress-dynamic-join Disable
```

Obr. 5.2: Výpis nastavení na prepínači Huawei

```
Switch#sh ip igmp snooping vlan 100
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 100:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
```

Obr. 5.3: Výpis nastavení na prepínači Cisco

Po spustení multicastového vysielania nahliadal prepínač do paketov a vedel identifikovať čo sa za ktorým rozhraním nachádza. Na obrázku 5.4 vidíme, že prepínač Huawei

identifikoval za rozhraním GE0/0/1 smerovač.

```
[HUswitch]dis igmp-snooping router-port vlan 100
 Port Name                       UpTime        Expires       Flags
 ----------------------------------------------------------------------
 VLAN 100, 1 router-port(s)
 GE0/0/1                         00:18:05      00:01:22      DYNAMIC
```

Obr. 5.4: Výpis router portu na prepínači Huawei

Rovnako správne identifikoval rozhranie so smerovačom aj prepínač od firmy Cisco, čo dokladá obrázok 5.5.

```
Switch#sh ip igmp snooping mrouter
Vlan    ports
----    -----
 100    Fa0/1(dynamic)
```

Obr. 5.5: Výpis router portu na prepínači Cisco

Počas testovania boli na prepínačoch pripojené viaceré stanice, pričom do multicastovej skupiny bola pripojená vždy len jedna. Toto bolo za účelom odsledovania, či prepínač naozaj bude preposielať správy len na porty, na ktorých sa nachádza posluchač. V oboch prípadoch prepínače správne identifikovali rozhranie ako ukazujú obrázky 5.6 a 5.7.

```
[HUswitch]dis igmp-snooping port-info
 ----------------------------------------------------------------------
                   (Source, Group)  Port                          Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------
 VLAN 100, 2 Entry(s)
                   (*, 224.0.1.40)  GE0/0/1                       -D-
                                                  1 port(s)
                    (*, 239.0.0.1)  GE0/0/24                      -D-
                                                  1 port(s)
 ----------------------------------------------------------------------
```

Obr. 5.6: Informácie o portoch na prepínači Huawei

Na obrázku 5.6 vidíme, že prepínač od firmy Huawei identifikoval na porte GE0/0/24 príjemcu multicastovej skupiny 239.0.0.1. Na port GE0/0/1 prichádzal multicast s adresou 224.0.1.40 preto si túto informáciu zaradil do tabuľky a v prípade, že by sa objavil multicast adresovaný tejto skupine, tak by preposlal dáta na tento port. Táto adresa však pri tejto konfigurácii nehrala žiadnu úlohu. Poukazuje len na fakt, že smerovač od firmy

Cisco, ktorý bol za týmto portom pripojený, vystupuje v základnej konfigurácii ako mapovací agent pre Auto-RP (cisco proprietarny protokol).

```
Switch#sh ip igmp snooping groups
Vlan      Group                Type        Version     Port List
------------------------------------------------------------------
100       239.0.0.1            igmp        v2          Fa0/1, Fa0/23
```

Obr. 5.7: Informácie o portoch na prepínači Cisco

Na obrázku 5.7 vidíme, že prepínač od spoločnosti Cisco identifikoval účastníkov multicastovej komunikácie za portami Fa0/1 (router port) a Fa0/23. V oboch výpisoch rovnako vidíme, že tieto porty boli oba v jednej VLANe (Vlan 100).

Ako som už spomínal v úvode, sledoval som funkcionalitu IGMP Snoopingu ako pri PIM-SM tak pri PIM-DM. Pri PIM-SM v podstate nieje v jeho činnosti nič, čo by mohlo komplikovať prípadne narušiť beh IGMP Snoopingu. Zaujímavejšie je to u PIM-DM. Tento protokol naplavuje na začiatku svojej činnosti multicast do všetkých častí siete, až kým sa neukáže, že v daných vetvách nie je o multicast záujem. To znamená, že v prípade kedy by nahliadanie do paketov nefungovalo korektne, dostával by sa aj na tie porty kde to nemá cenu.

Na obrázku 5.8 je ukážka odchytenej komunikácie zo stanice, ktorá nebola prihlásená k odberu multicastu. Vidíme, že tu zdrojová stanica s adresou 50.0.0.2 vysiela multicast pre skupinu 239.0.0.1. Obrázok ukazuje, že prešli len dva UDP pakety, zatiaľ čo na prijímacej stanici bežal príjem.

```
988 877.530237 10.0.0.1    224.0.0.5     OSPF      90 Hello Packet
989 887.529883 10.0.0.1    224.0.0.5     OSPF      90 Hello Packet
990 889.024871 50.0.0.2    239.0.0.1     UDP     1370 Source port: 49433  Destination port: 5004
991 889.044202 50.0.0.2    239.0.0.1     UDP     1370 Source port: 49433  Destination port: 5004
992 890.929793 10.0.0.1    224.0.0.13    PIMv2     68 Hello
993 897.529547 10.0.0.1    224.0.0.5     OSPF      90 Hello Packet
994 907.529184 10.0.0.1    224.0.0.5     OSPF      90 Hello Packet
```

Obr. 5.8: Záznam komunikácie na neprijímanej stanici

Podobne to vyzeralo pri využití prepínača Cisco aj Huawei. Vždy prešlo len pár paketov a preposielanie na neprijímací port bolo zastavené. To poukazuje na to, že medzi oboma zariadeniami funguje snooping bez problémov.

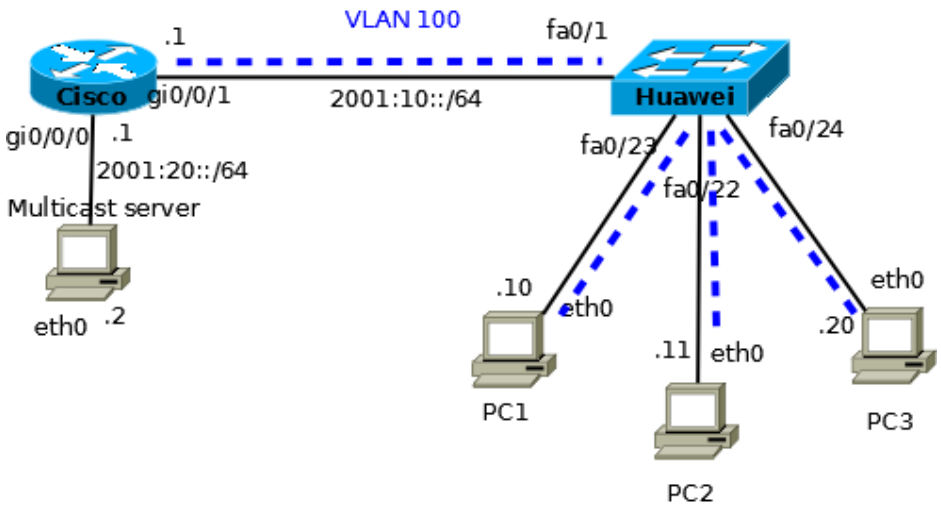
# 6 Konfigurácia MLD Snooping

Zariadenia od firmy Huawei, ktoré sú dostupne v škole sú totiž dodávané s firmware V200R003C00SPCXXX (namiesto xxx je trojčíslie, ktoré sa na nich mení v závislosti na konkrétnom zariadení). Tento firmware však nepodporuje IPv6 multicast a teda ani MLD či MLD Snooping. Z toho dôvodu, som musel vyjednať s obchodným zástupcom tejto spoločnosti nový firmware. Upgrade bol vykonaný na jednom smerovači a jednom prepínači a to na verziu V200R005C00SPCXXX. Na prepínači Cisco Catalyst 2960 bolo zase za účelom povolenia IPv6 nutné spustiť duálny mód (sdm prefer dual-ipv4-and-ipv6 default).

Rovnako ako pri IGMP snoopingu testovanie prebehlo v oboch variantach (Cisco smerovač- Huawei prepínač, Huawei smerovač - Cisco prepínač). Použité zariadenia boli taktiež totožné ako pri IGMP snoopingu.

## 6.1 Nastavenia prepínačov

Sieť bola zapojená podľa obrázku 6.1. Podobne ako pri IGMP Snoopingu pomenovania aktívnych prvkov v tejto schéme sú len ilustračné. Ostatné informácie v topológii sú rovnaké pri oboch variantách zapojenia.




Obr. 6.1: Topológia siete pre MLD Snooping

Konfigurácia MLD Snoopingu na prepínači Cisco vyzerá následovne:

- Aktivácia MLD Snoopingu
  - *switch(config)# ipv6 mld snooping*
- Vstup do konfiguračného moodu pre VLAN, v ktorej chceme MLD Snooping využívať
  - *switch(config)# vlan <vlan-id>*
- Povolenie MLD Snoopingu pre danú VLAN
  - *switch(config-vlan)# ipv6 mld snooping*

Na prepínači od spoločnosti Huawei je konfigurácia nasledovná:

- Aktivácia MLD Snoopingu
  - *[switch]mld-snooping enable*
- Vstup do konfiguračného moodu pre VLAN, v ktorej chceme MLD Snooping využívať
  - *[switch] vlan <vlan-id>*
- Povolenie MLD Snoopingu pre danú VLAN
  - *[switch-vlan]mld-snooping enable*
- Nastavenie verzie MLD snoopingu
  - *[switch-vlan]mld-snooping version 2*

Skrátené konfigurácie prepínačov sa nachádzajú v prílohách (Prílohy) F.2 pre Cisco a F.1 pre Huawei. Nakoľko sa jedná v podstate o ekvivalent IGMP Snoopingu, ktorý pracuje nad IPv6 platí aj tu, že popis konfigurácie smerovačov nebudem v tejto kapitole popisovať pretože protokol PIMv6 (známy aj ako IPv6 PIM) je rozobraný v samostatnej kapitole.

## 6.2 Overenie funkčnosti konfigurácie

Po prvom nakonfigurovaní fungoval MLD snooping len na prepínači od firmy Cisco. Prepínač od spoločnosti Huawei rozosielal multicast na všetky porty akoby to bol broadcast. Po preskúmaní nastavení MLD Snoopingu obrázok 6.2 sa ukázalo, že síce je aktívny avšak vo verzii 1 pričom smerovač pracoval na verzii 2. Po prenastavení začal pracovať MLD snooping správne aj na zariadení od firmy Huawei. Nastavenia MLD Snoopingu z prepínača od spoločnosti Cisco sú na obrázku 6.3.

```
[Quidway]display mld-snooping vlan 100
 MLD Snooping Vlan Information for VLAN 100
     MLD Snooping is Enabled
     MLD Version is Set to default 1
     MLD Query Interval is Set to default 125s
     MLD Max Response Interval is Set to default 10s
     MLD Robustness is Set to default 2
     MLD Last Member Query Interval is Set to default 1s
     MLD Router Port Aging Interval is Set to 180s or holdtime in hello
     MLD Filter Group-Policy is not set
     MLD Prompt Leave Disable
     MLD Router Alert is Not Required
     MLD Send Router Alert Enable
     MLD Snooping proxy is disabled
     MLD Snooping report-suppress is disabled
     MLD Snooping Querier is disabled
```

Obr. 6.2: Výpis nastavení na prepínači Huawei

```
Switch#sh ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
----------------------------------------
MLD snooping                : Enabled
MLDv2 snooping (minimal)    : Enabled
Listener message suppression : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Robustness variable         : 2
Last listener query count   : 2
Last listener query interval : 1000

Vlan 100:
--------
MLD snooping                        : Enabled
MLD immediate leave                 : Disablec
Robustness variable                 : 2
Last listener query count           : 2
Last listener query interval        : 1000
```

Obr. 6.3: Výpis nastavení na prepínači Cisco

Po spustení multicastu začali prepínače nahliadať do paketov a ukladať si informácie o portoch na ktorých sa objavoval. Prepínač od firmy Cisco správne identifikoval že na portoch F0/1 (router port) a Fa0/23 prebieha multicastový prenos pre skupinu FF05::1:4. Tento prepínač však zachytil aj inú adresu a to FF02:FB na všetkých aktívnych portoch. Táto adresa je priradená k mDNS (multicast Domain Name System) a zobrazuje sa tu pravdepodobne z dôvodu, že som pri testovaní používal počítače s operačným systémom Linux, ktorý používa nss-mdns službu. V tejto službe je zahrnutý prave mDNS (viac informácii RFC 6762).

```
Switch#show ipv6 mld snooping address
Vlan      Group                Type        Version     Port List
------------------------------------------------------------------------------
100       FF02::FB             mld         v2          Fa0/1, Fa0/23,
                                                       Fa0/24
100       FF05::1:4            mld         v2          Fa0/1, Fa0/23
```

Obr. 6.4: Informácie o portoch na prepínači Cisco

Správne identifikoval komunikáciu aj prepínač od spoločnosti Huawei. Ako ukazuje obrázok 6.5 port GE0/0/1 je pripojený k smerovaču a spolu s portom GE0/0/23 účastníkom multicastovej komunikácie pre skupinu FF05::1:4.

```
[Quidway]display mld-snooping forwarding-table vlan 100
VLAN ID : 100, Forwarding Mode : IP
--------------------------------------------------------------------------------
                          (Source, Group)   Interface                Out-Vlan
--------------------------------------------------------------------------------
                                Router-port   GigabitEthernet0/0/1        100
                    (*, ff05:0:0:0:0:0:1:4)   GigabitEthernet0/0/1        100
                                              GigabitEthernet0/0/23       100
--------------------------------------------------------------------------------
Total Group(s) : 1
```

Obr. 6.5: Informácie o portoch na prepínači Huawei

Z dôvodu, že PIMv6 v hustom režime nie je na zariadeniach Cisco implementovaný, nebolo možné otestovať ako sa prepínač od firmy Huawei postará o elimináciu naplavovania (situácia ako v kapitole o IGMP snoopingu). Avšak, pre prepínač Cisco to možné bolo, nakoľko smerovač od spoločnosti Huawei touto funkcionalitou disponuje. Na obrázku 6.6 vidíme záznam z neprijímajúcej stanice, z ktorého je jasné, že rovnako ako pri IGMP snoopingu po pár paketoch prestane switch na tento port preposielať multicast. Rovnako si môžeme všimnúť, že (ako sa spomína v teoretickej časti práce) MLD je skutočne zahrnuté do ICMPv6.

```
Cisco_52:40:1a      Spanning-tree-(for-STP          60 Conf. Root = 32768/100/00:25:46:52:40:00
fe80::76d4:35ff:fe7 ff02::16          ICMPv6        90 Multicast Listener Report Message v2
2001:20::1          ff05::1:4         UDP           85 Source port: 35595  Destination port: 5024
Cisco_52:40:1a      Spanning-tree-(for-STP          60 Conf. Root = 32768/100/00:25:46:52:40:00
2001:20::1          ff05::1:4         UDP           85 Source port: 35595  Destination port: 5024
fe80::a19:a6ff:fe9b ff02::d           PIMv2        114 Hello
```

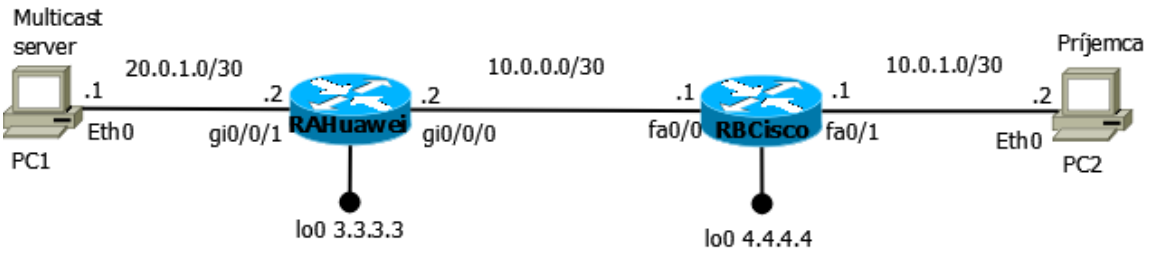
Obr. 6.6: Záznam komunikácie na neprijímacej stanici

# 7 Konfigurácia PIM DM

Na začiatok je nutné mať funkčné unicastové smerovanie (jeho nastaveniu sa venovať nebudem). Ja som pri testovaní používal smerovací protokol OSPF, ale na tom pri protokole PIM nezáleží. Konfigurácia prebieha na smerovačoch od rôznych výrobcov. Smerovač s názvom RAHuawei je od firmy Huawei (model AR3260) a smerovač s názvom RBCisco je od firmy Cisco (model 2800) (viď obr.7.1).

## 7.1 Nastavenia smerovačov

Sieť bola zapojená podľa topológie (viď obr.7.1).




Obr. 7.1: Topológia siete pre PIM SM/DM

Konfigurácia prvkov Cisco a Huawei je mierne odlišná. Na smerovači Cisco[15] vyzerá konfigurácia následovne:

- Povolenie multicástoveho smerovania
  - *Router(config)# ip multicast-routing*
- Na rozhraní, na ktorom chceme povoliť protokol PIM DM
  - *Router(config-if)# ip pim dense-mode*

Konfigurácia smerovača RBCisco je v prílohe B.2 (Prílohy).

Na smerovači Huawei je konfigurácia nasledovná:

- Povolenie multicástoveho smerovania
  - *[Router]multicast routing-enable*

- Na rozhraní, na ktorom chceme povoliť protokol PIM DM
  - *[Router-GigabitEthernet0/0/0]pim dm*
- Na rozhraní vedúcom k užívatelskej stanici (alebo multicast servru)
  - *[Router-GigabitEthernet0/0/1]igmp enable*

Konfigurácia smerovača RAHuawei je v prílohe B.1 (Prílohy).

## 7.2 Overenie funkčnosti konfigurácie

Po spustení multicastového vysielania sa zo zdroja začal multicast šíriť, o čom svedčí výpis z multicastovej smerovacej tabuľky. Na obrázku 7.2 vidíme výpis zo smerovača Cisco. Jeho druhý záznam nasvedčuje, že z rozhrania FastEthernet0/0 prichádza multicastové vysielanie, ktoré je ďalej smerované na rozhranie FastEthernet0/1 v Dense mode.

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.0.0.1), 00:01:14/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/1, Forward/Dense, 00:01:08/00:00:00
    FastEthernet0/0, Forward/Dense, 00:01:14/00:00:00

(20.0.1.1, 239.0.0.1), 00:01:14/00:02:59, flags: T
  Incoming interface: FastEthernet0/0, RPF nbr 10.0.0.2
  Outgoing interface list:
    FastEthernet0/1, Forward/Dense, 00:01:08/00:00:00

(*, 224.0.1.40), 00:01:35/00:02:19, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/0, Forward/Dense, 00:01:35/00:00:00
    Loopback0, Forward/Dense, 00:01:35/00:00:00
```

Obr. 7.2: Výpis multicastovej smerovacej tabuľky Cisco

Výpis zo smerovača Huawei je o niečo chudobnejší (viď obr. 7.3). Neobsahuje systémové záznamy, ktoré súvisia s behom protokolu PIM, ale len záznam o užívateľom

vytvorenom prenose. Na obrázku je vidieť, podobne ako u Cisca, z ktorého rozhrania vysielanie prichádza a ktorým rozhraním opúšťa smerovač.

```
Multicast routing table of VPN-Instance: public net
 Total 1 entry

 00001. (20.0.1.1, 239.0.0.1)
       Uptime: 00:02:26
       Upstream Interface: GigabitEthernet0/0/1
       List of 1 downstream interface
           1:  GigabitEthernet0/0/0
```

Obr. 7.3: Výpis multicastovej smerovacej tabuľky Huawei

Na obrázku 7.4 vidíme výpis debugingu na smerovači Cisco. Výpis zobrazuje proces zostavenia komunikácie. Na začiatku vloží záznam o vysielaní z 20.0.1.1 do skupiny 239.0.0.1, ktorá je dostupná za adresou 10.0.0.2 do fronty. Pripravý si Join/Prune paket pre suseda s adresou 10.0.0.2. Do tohto paketu prídá správu Join pre spomínanú skupinu a odošle. V posledom riadku vidíme, že sa snažil zostaviť obnovenie prerezaných vetví (graft), avšak nenašiel o takýchto príjemcoch žiadny záznam.

```
*Jan 23 11:42:36.523: PIM(0): Insert (20.0.1.1,239.0.0.1) join in nbr 10.0.0.2s queue
*Jan 23 11:42:36.523: PIM(0): Building Triggered (*,G) Join / (S,G,RP-bit) Prune message for
    239.0.0.1
*Jan 23 11:42:36.523: PIM(0): Building Join/Prune packet for nbr 10.0.0.2
*Jan 23 11:42:36.523: PIM(0): Adding v2 (20.0.1.1/32, 239.0.0.1), S-bit Join
*Jan 23 11:42:36.523: PIM(0): Send v2 join/prune to 10.0.0.2 (FastEthernet0/0)
*Jan 23 11:42:36.543: PIM(0): Building Graft message for 239.0.0.1, FastEthernet0/1: no entries
```

Obr. 7.4: Výpis debugingu protokolu PIM zo smerovača Cisco

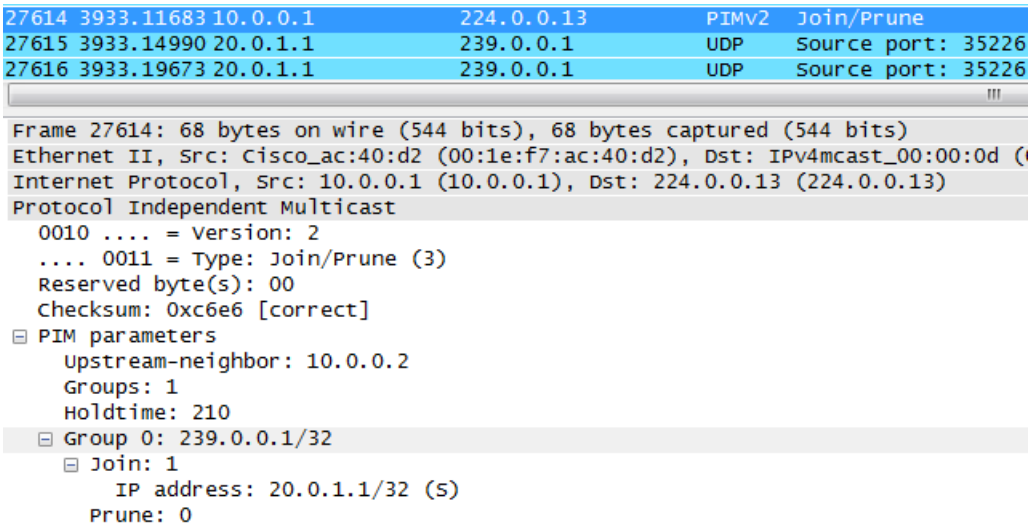
Na obrázku 7.5 vidíme výpis z debugu na smerovači Huawei. Zo správ vidíme, že obdržal správu so žiadosťou o pripojenie z IP adresy 10.0.0.1. Zareaguje tak, že rozhranie s adresou 10.0.0.2 nastaví ako vysielacie rozhranie. Pre skupinu 239.0.0.1 čaká jedno pripojenie a žiadne prerezanie vetví. Z adresy 20.0.1.1 obdržal žiadosť o pridanie do skupiny. Túto adresu priradil ako IP príjemcu pre multicastovú skupinu 239.0.0.1. Vo výpisoch vidíme, že táto adresa bola pôvodne v zozname prerezaných (pruned). Pretože obdržal

správu Join presunul ju do zoznamu NoInfo a zrušil odpočet pretože aktuálne je táto stanica prijímajúca.

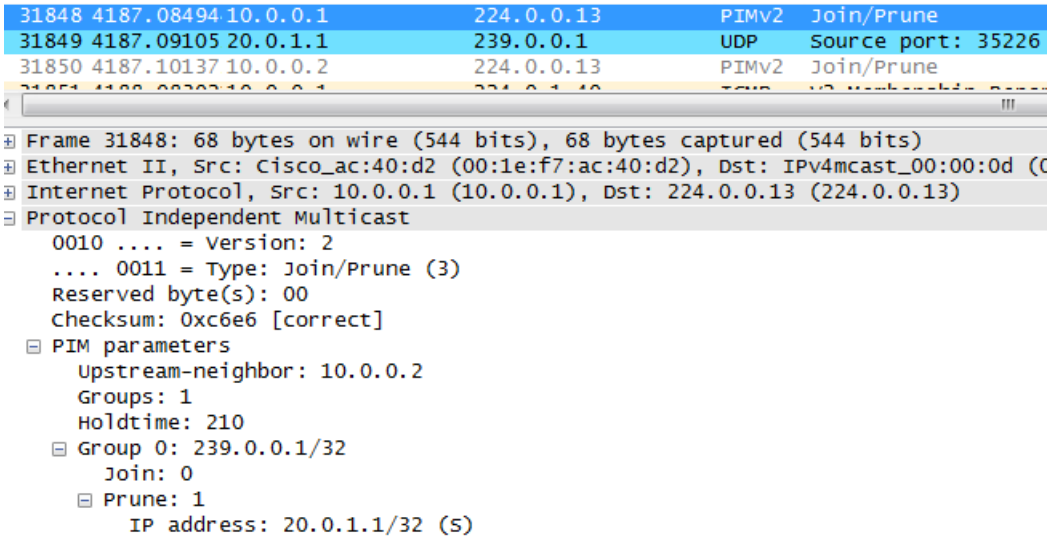
```
Jan 23 2015 20:29:18.60.1+00:00 3200 PIM/7/JP:(public net): PIM ver 2 JP receiving 10.0.0.1 -> 224.0.0.13 on GigabitEthernet0/0/0 (P013091)
Jan 23 2015 20:29:18.60.2+00:00 3200 PIM/7/JP:(public net): Upstream 10.0.0.2, Groups 1, Holdtime 210 (P013097)
Jan 23 2015 20:29:18.60.3+00:00 3200 PIM/7/JP:(public net): Group: 239.0.0.1/32 --- 1 join 0 prune (P013107)
Jan 23 2015 20:29:18.60.4+00:00 3200 PIM/7/JP:(public net): Join: 20.0.1.1/32 S (P013117)
Jan 23 2015 20:29:18.60.5+00:00 3200 PIM/7/EVENT:(public net): PIM-DM: Downstream (20.0.1.1, 239.0.0.1) FSM current state: Pruned, event: 2 (D07503)
Jan 23 2015 20:29:18.60.6+00:00 3200 PIM/7/EVENT:(public net): PIM-DM: Downstream (20.0.1.1, 239.0.0.1) on interface GigabitEthernet0/0/0 (10.0.0.2) FSM transited from Pruned to NoInfo. Join Received (D07)
Jan 23 2015 20:29:18.60.7+00:00 3200 PIM/7/EVENT:(public net): Prune timer for (20.0.1.1,239.0.0.1) on GigabitEthernet0/0/0 cancelled (D071042)
```

Obr. 7.5: Výpis debugingu protokolu PIM zo smerovača Huawei

Vo výpisoch zachytenej komunikácie, ktorá prebiehala medzi smerovačmi môžeme vidieť, ako smerovač Cisco žiada o pripojenie do skupiny 239.0.0.1 (viď obr 7.6). Správa je odoslaná zo zdrojovej adresy 10.0.0.1 na adresu 224.0.0.13, na ktorej počúvajú všetky smerovače s nastaveným protokolom PIMv2. V prípade, že v jeho vetvách už nie je žiadny príjemca pre danú skupinu, pošle správu so žiadosťou o prerezanie (viď obr 7.7).




Obr. 7.6: Ukážka správy join




Obr. 7.7: Ukážka správy Prune

# 8 Konfigurácia PIM SM

Protokol PIM SM podobne ako dense mode vyžaduje funkčné unicastove smerovanie. U tohto protokolu je viac možností ako sa dá určiť rendevouz point. Základným spôsobom je pevné nadefinovanie RP a teda jeho statické umiestnenie. Ďalším spôsobom je možnosť automatickej voľby RP kedy smerovače zvolia RP. A posledným spôsobom je nastavenie dvoch RP staticky, pričom sú prepojené pomocou MSDP tzv. Anycast RP. Možnosti automatického RP a Anycast RP sa využívajú ako systém ochrany RP pred výpadkom, nakoľko po výpadku smerovača, ktorý figuruje ako rendevouz point prevezme jeho úlohu iný.

Možnosť Anycast RP je v tomto ohľade rýchlejšia, nakoľko oba RP majú rovnaké informácie a ak jeden z nich vypadne na komunikácii sa tento výpadok nijako neprejaví. Pri automatickom zvolení RP bude komunikácia na krátko pozastavená, respektíve pakety nebudú doručované cieľovým staniciam, pretože musí prebehnúť prepnutie na RP kandidáta.

## 8.1 Nastavenia pre statický RP

Táto konfigurácia sa oproti Dense mode líši len minimálne. Hlavným rozdielom je, že sparse mode potrebuje k funkcii RP. Topológia siete bola preto rovnaká (viď obr.7.1). Na smerovači Cisco vyzerá konfigurácia následovne:

- Povolenie multicástoveho smerovania
  - *Router(config)# ip multicast-routing*
- Na rozhraní, na ktorom chceme povoliť protokol PIM SM
  - *Router(config-if)# ip pim sparse-mode*
- Nastavenie statickej adresy RP
  - *Router(config)# ip pim rp-address <adresa RP>*

Konfigurácia smerovača RBCisco je v prílohe C.2 (Prílohy).

Na smerovači Huawei je konfigurácia nasledovná:

- Povolenie multicástoveho smerovania

  - *[Router]multicast routing-enable*

- Na rozhraní, na ktorom chceme povoliť protokol PIM SM
  - *[Router-GigabitEthernet0/0/0]pim sm*
- Na rozhraní vedúcom k užívateľskej stanici (alebo multicast servru)
  - *[Router-GigabitEthernet0/0/1]igmp enable*
- Nastavenie statickej adresy RP
  - *[Router]pim*
  - *[Router-pim]static-rp <adresa RP>*

Konfigurácia smerovača RAHuawei je v prílohe C.1 (Prílohy).

## 8.2 Overenie funkčnosti konfigurácie so statickým RP

Prenos multicastu fungoval správne. V uvedených výpisoch je ako RP nastavený smerovač od firmy Huawei. Skúšal som aj variantu s RP na smerovači Cisco, ale na funkcionalitu to nemalo žiadny dopad a vo výpisoch by sa to prejavilo len rozdielnou adresou RP. Ako adresy RP som využíval loopback rozhrania pre jednoznačnejšie orientovanie v topológiach. Na obrázku 8.1 je výpis zo smerovača Cisco, na ktorom vidíme obdobné informácie ako pri PIM DM. Rozdielne je, že v záznamoch je nami nastavená adresa rendevouz pointu (RP 3.3.3.3). Z obrázka tiež vidíme, že sa jedná o sparse prenos (Forward/Sparse).

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.0.0.1), 00:01:49/stopped, RP 3.3.3.3, flags: SJC
  Incoming interface: FastEthernet0/0, RPF nbr 10.0.0.2
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:01:49/00:02:28

(20.0.1.1, 239.0.0.1), 00:01:49/00:02:12, flags: JT
  Incoming interface: FastEthernet0/0, RPF nbr 10.0.0.2
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:00:47/00:02:28

(*, 224.0.1.40), 00:12:18/00:02:42, RP 3.3.3.3, flags: SJPL
  Incoming interface: FastEthernet0/0, RPF nbr 10.0.0.2
  Outgoing interface list: Null
```

Obr. 8.1: Výpis multicastovej smerovacej tabuľky Cisco

Záznam v multicastovej smerovacej tabuľke Huawei neobsahuje dostatok informácii, aby sa dalo tvrdiť, že funguje správne (viď obrázok 8.2). Detailnejšie záznamy sú u Huawei až v smerovacej tabuľke protokolu PIM (*display pim routing-table*).

```
Multicast routing table of VPN-Instance: public net
 Total 1 entry

 00001. (20.0.1.1, 239.0.0.1)
       Uptime: 00:03:28
       Upstream Interface: GigabitEthernet0/0/1
       List of 1 downstream interface
           1:  GigabitEthernet0/0/0
```

Obr. 8.2: Výpis multicastovej smerovacej tabuľky Huawei

V smerovacej tabuľke protokolu PIM (viď obrázok 8.3) vidíme obdobné informácie ako je tomu u smerovača Cisco. V každom zázname sa uvádza aj adresa RP, pričom v tomto konkrétnom prípade je v zátvorke local čo značí, že rendevouz pointom je práve tento smerovač.

```
<3200>disp pim routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 239.0.0.1)
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:00:25
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/0
             Protocol: pim-sm, UpTime: 00:00:25, Expires: 00:03:05

 (20.0.1.1, 239.0.0.1)
     RP: 3.3.3.3 (local)
     Protocol: pim-sm, Flag: SPT 2MSDP LOC ACT
     UpTime: 00:01:04
     Upstream interface: GigabitEthernet0/0/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/0
             Protocol: pim-sm, UpTime: 00:00:25, Expires: 00:03:05
```

Obr. 8.3: Výpis PIM smerovacej tabuľky Huawei

Na obrázku 8.4 vidíme záznam z debugu smerovača Cisco. V tomto zázname vidíme, že overuje adresu 3.3.3.3 ako RP v skupine 239.0.0.1 a aj v skupine 224.0.1.40 (túto adresu používa cisco ako auto-rp discovery). Potom je zrejnmé, že žiada o pripojenie k multicastovej skupine 239.0.0.1 prostredníctvom susedného smerovača s IP 10.0.0.2. Rovnako ako tomu bolo aj u PIM-DM. Hlavným rozdielom však je že do Join/Prune paketu pridáva aj žiadosť o pripojenie RP (3.3.3.3) k skupine 239.0.0.1.

```
*Jan 23 11:24:23.895: PIM(0): Check RP 3.3.3.3 into the (*, 239.0.0.1) entry
*Jan 23 11:24:23.895: PIM(0): Check RP 3.3.3.3 into the (*, 224.0.1.40) entry
*Jan 23 11:25:25.375: PIM(0): Insert (20.0.1.1,239.0.0.1) join in nbr 10.0.0.2s queue
*Jan 23 11:25:25.375: PIM(0): Building Triggered (*,G) Join / (S,G,RP-bit) Prune message for
    239.0.0.1
*Jan 23 11:25:25.379: PIM(0): Insert (*,239.0.0.1) join in nbr 10.0.0.2's queue
*Jan 23 11:25:25.379: PIM(0): Building Join/Prune packet for nbr 10.0.0.2
*Jan 23 11:25:25.379: PIM(0): Adding v2 (3.3.3.3/32, 239.0.0.1), WC-bit, RPT-bit, S-bit Join
*Jan 23 11:25:25.379: PIM(0): Adding v2 (20.0.1.1/32, 239.0.0.1), S-bit Join
*Jan 23 11:25:25.379: PIM(0): Send v2 join/prune to 10.0.0.2 (FastEthernet0/0)
```

Obr. 8.4: Výpis z debugu protokolu PIM na smerovači Cisco

Na obrázku 8.5 vidíme obdobný debug zo smerovača Huawei, ktorý bol v úlohe RP. Tento smerovač dosáva pre skupinu 239.0.0.1 dve správy Join a 0 Prune. Prvý join je na adresu 3.3.3.3 a druhý na adresu 20.0.1.1. V ďalšom riadku vidíme, že pre PIM-SM sa vytvorý nový záznam v multicastovej smerovacejtabulke.

```
Jan 23 2015 20:20:14.990.3+00:00 3200 PIM/7/JP:(public net): Group: 239.0.0.1/32 --- 2 joins 0
    prune (P013107)
Jan 23 2015 20:20:14.990.4+00:00 3200 PIM/7/JP:(public net): Join: 3.3.3.3/32 SWR (P013117)
Jan 23 2015 20:20:14.990.5+00:00 3200 PIM/7/JP:(public net): Join: 20.0.1.1/32 S (P013117)
Jan 23 2015 20:20:14.990.6+00:00 3200 PIM/7/ROUT:(public net): PIM-SM: Create (*, 239.0.0.1)
    entry in mrt. (S0117412)
```

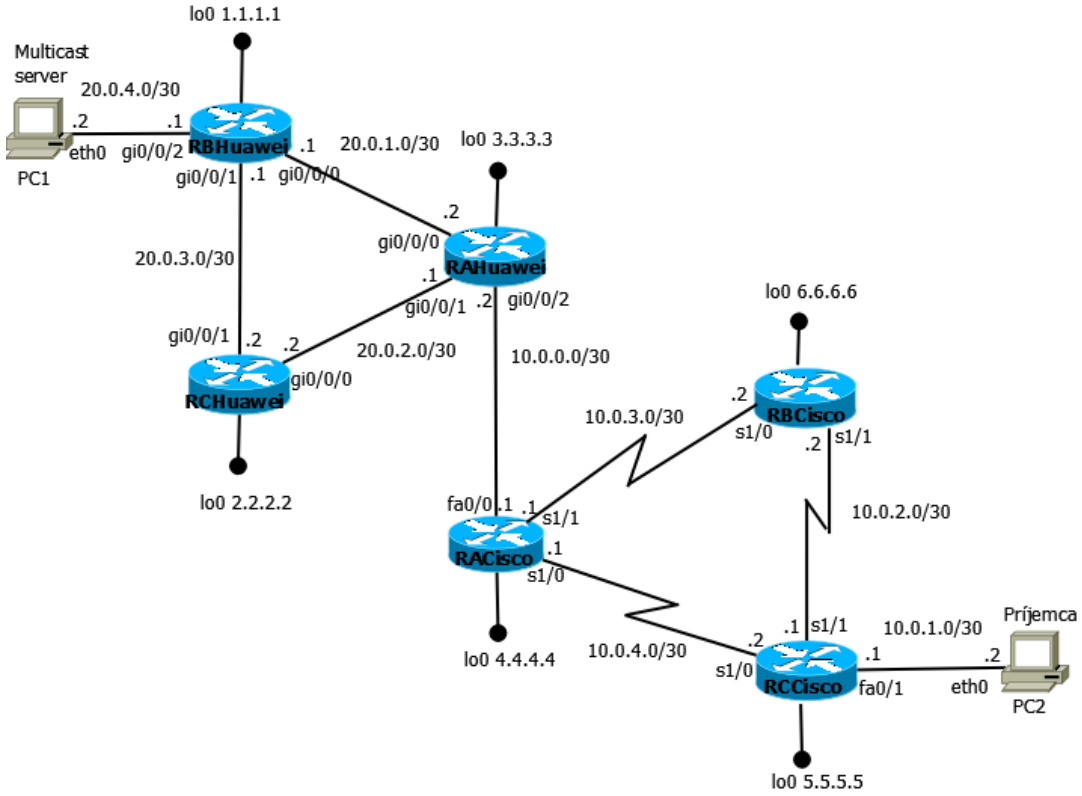
Obr. 8.5: Výpis z debugu protokolu PIM na smerovači Huawei

Výpis zo zachytenej komunikácie je v podstate totožný s výpisom uvedenom pri PIM DM (obr. 7.6 a obr. 7.7). Rozdiel je len v tom ako prebieha prenos. Pri PIM DM je od začiatku multicast rozosielaný do všetkých častí siete aj tam, kde nie je o príjem záujem a postupne sa vetvy bez poslucháčov prerežú (prune). Pri SM je to presne naopak. Pokiaľ nie sú definovaný príjemcovia pre danú skupinu, multicast nie je šírený do žiadnych vetiev.

## 8.3 Nastavenia pre automatickú voľbu RP

Pri tomto zapojení som vychádzal z topológie uvedenej na obrázku 8.6. Najskôr som sledoval ako sa zachovajú pri vyhodnocovaní RP a BSR smerovače jednotlivých výrobcov medzi sebou. Takže smerovače RAHuawei a RACisco boli rozpojené. Po spojení som zvolený RP a BSR znova skontroloval.

Konfigurácia smerovačov vychádza zo základnej konfigurácie PIM SM takže je nutné, aby bolo zabezpečené unicastové smerovanie. Taktiež zapnutie multicastoveho smerovania a protokolu PIM SM na jednotlivých rozhraniach zostáva nezmenený, preto tento postup v tejto časti znova neuvádzam.




Obr. 8.6: Topológia siete pre PIM SM Auto RP

Hlavný rozdiel voči predchádzajúcej konfigurácii je v nastavení RP. Nastavenie smerovača Cisco pre automatické zvolenie RP vyzeralo nasledovne:

- Nastavenie kandidáta na RP (doporučujem použiť loopback rozhranie)

  - *Router(config)#ip pim rp-candidate <rozhranie>*

- Nastavenie kandidáta na BSR (rovnako doporučujem loopback rozhranie)

  - *Router(config)#ip pim bsr-candidate <rozhranie>*

Výpisy konfigurácii pre jednotlivé smerovače Cisco sa nachádzajú v prílohe D.4,D.5 a D.6 (Prílohy).

Na nastavenie smerovačov Huawei som použil nasledovné príkazy:

- Vstup do konfigurácie PIM

  - *[Router]pim*

- Nastavenie kandidáta na RP (doporučujem použiť loopback rozhranie)

  - *[Router-pim]c-rp <rozhranie>*

- Nastavenie kandidáta na BSR (rovnako doporučujem loopback rozhranie)

  - *[Router-pim]c-bsr <rozhranie>*

Výpisy konfigurácii pre jednotlivé smerovače Huawei sa nachádzajú v prílohách D.1,D.2 a D.3 (Prílohy).

## 8.4 Overenie funkčnosti konfigurácie automatickej voľby RP

V situácii, kedy boli jednotlivé časti siete oddelené prebiehala voľba RP rôzne. V sieti Cisco smerovačov bol ako BSR zvolený kandidát s adresou 6.6.6.6 (viď obrázok 8.7). Kandidát na BSR v prípade výpadku má adresu 4.4.4.4. Za RP bol zvolený smerovač s rovnakou adresou ako BSR (viď obrázok 8.8)

```
R3#sh ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 6.6.6.6 (?)
  Uptime:      01:51:00, BSR Priority: 0, Hash mask length: 0
  Expires:     00:01:45
This system is a candidate BSR
  Candidate BSR address: 4.4.4.4, priority: 0, hash mask length: 0
  Candidate RP: 4.4.4.4(Loopback0)
    Holdtime 150 seconds
    Advertisement interval 60 seconds
    Next advertisement in 00:00:00
```

Obr. 8.7: Výpis zobrazujúci informácie o BSR na smerovači RACisco

```
R3#sh ip pim rp
Group: 239.0.0.1, RP: 6.6.6.6, v2, uptime 01:46:38, expires 00:02:23
```

Obr. 8.8: Výpis zobrazujúci informácie o RP na smerovači RACisco

Táto situácia nie je vhodná, pretože v prípade výpadku tohto smerovača by museli prebehnúť dve vyhodnocovania súčasne, pretože by sieť v jednom okamihu prišla aj o RP aj o BSR.

U siete Huawei to vyzeralo o niečo logickejšie. Ako BSR bol zvolený smerovač s adresou 3.3.3.3 (viď obrázok8.9) a kandidátom je smerovač s adresou 1.1.1.1 (smerovač sám). Ako RP bol zvolený smerovač s adresou 1.1.1.1 (viď obrázok 8.10).

```
<Huawei>dis pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 3.3.3.3
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 00:10:17
     Expires: 00:01:17
     C-RP Count: 3
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: 1.1.1.1
     Priority: 0
     Hash mask length: 30
     State: Candidate
     Scope: Not scoped
     Wait to be BSR: 0
```

Obr. 8.9: Výpis zobrazujúci informácie o BSR na smerovači RBHuawei

```
<Huawei>dis pim rp-info 239.0.0.1
 VPN-Instance: public net
 BSR RP Address is: 1.1.1.1
     Priority: 0
     Uptime: 01:38:49
     Expires: 00:01:50
 RP mapping for this group is: 1.1.1.1 (local host)
```

Obr. 8.10: Výpis zobrazujúci informácie o RP na smerovači RBHuawei

U Huawei bolo nutné vypísať RP pre konkrétnu adresu skupiny, pretože pri výpise *display pim rp-info* sa zobrazia všetci možný kandidáti na RP. To môže byť spôsobené tým, že Huawei nedoporučuje plne automatické vyjednanie RP. Automatická voľba má prebiehať len v prípade výpadku a preto sa predpokladá, že bude RP určený staticky.

Po spojení týchto dvoch sietí prebehlo znovu vyjednanie BSR a RP. Ako BSR bol vybraný smerovač s adresou 6.6.6.6 (viď obrázok 8.11 a obrázok 8.12). V závislosti, na ktorom smerovači je tento výpis uskutočnený, je zobrazený kandidát. Jednotlivé smerovače navrhujú ako kandidáta vždy seba, pretože majú na seba samého najlepšiu dosažiteľnosť.

```
R3#sh ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 6.6.6.6 (?)
  Uptime:      03:06:09, BSR Priority: 0, Hash mask length: 0
  Expires:     00:01:58
This system is a candidate BSR
  Candidate BSR address: 4.4.4.4, priority: 0, hash mask length: 0
  Candidate RP: 4.4.4.4(Loopback0)
    Holdtime 150 seconds
    Advertisement interval 60 seconds
    Next advertisement in 00:00:51
```

Obr. 8.11: Informácie o BSR zo smerovača RACisco po spojení

```
<RAHuawei>dis pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 6.6.6.6
     Priority: 0
     Hash mask length: 0
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 00:00:06
     Expires: 00:02:05
     C-RP Count: 6
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: 3.3.3.3
     Priority: 0
     Hash mask length: 30
     State: Candidate
     Scope: Not scoped
     Wait to be BSR: 0
```

Obr. 8.12: Informácie o BSR zo smerovača RAHuawei po spojení

Ako RP bol vyjednaný smerovač podľa pôvodného výberu Cisca akurát sa rozšíril do všetkých častí siete, ako zobrazujú obrázky 8.13 a 8.14

```
R3#sh ip pim rp
Group: 239.0.0.1, RP: 6.6.6.6, v2, uptime 01:46:38, expires 00:02:23
```

Obr. 8.13: Informácie o RP zo smerovača RACisco po spojení

```
<RAHuawei>dis pim rp 239.0.0.1
 VPN-Instance: public net
 BSR RP Address is: 6.6.6.6
     Priority: 0
     Uptime: 00:21:37
     Expires: 00:01:58
 RP mapping for this group is: 6.6.6.6
```

Obr. 8.14: Informácie o RP zo smerovača RAHuawei po spojení

Princíp komunikácie zostáva nezmenený, preto sa skôr zameriam na spôsob výmeny informácii o RP a BSR. Vo výpise s debugu na smerovači RACisco (viď obr. 8.15) vidíme, že smerovač obdržal update od smerovačov, ktoré už poznal a Bootstrap zo svojich priamo pripojených rozhraní. Následne začal postupne pridávt nových kandidátov na RP. Najprv prišla správa od priamo pripojeného smerovača s IP 3.3.3.3. Túto adresu si zapamätal a začína od nej prijímať update. Rovnako to urobil aj s adresou 2.2.2.2 a 1.1.1.1. Z týchto informácii sú následne spočítané hodnoty hashov a podla nich zvolený RP. Popri tom neustále dostáva Bootstrap správy zo svojich rozhraní.

```
*Jan 23 12:53:29.067: PIM(0): Update (224.0.0.0/4, RP:6.6.6.6), PIMv2
*Jan 23 12:53:29.067: PIM(0): Update (224.0.0.0/4, RP:4.4.4.4), PIMv2
*Jan 23 12:53:29.067: PIM(0): Update (224.0.0.0/4, RP:5.5.5.5), PIMv2
*Jan 23 12:53:29.039: PIM(0): Received v2 Bootstrap on Loopback0 from 4.4.4.4
*Jan 23 12:53:29.047: PIM(0): Received v2 Bootstrap on Serial0/1/1 from 10.0.4.2
*Jan 23 12:53:29.067: PIM(0): Received v2 Bootstrap on Serial0/1/0 from 10.0.3.2
*Jan 23 12:53:29.067: PIM(0): Added with (224.0.0.0/4, RP:3.3.3.3), PIMv2
*Jan 23 12:53:29.079: PIM(0): Added with (224.0.0.0/4, RP:2.2.2.2), PIMv2
*Jan 23 12:53:29.039: PIM(0): Received v2 Bootstrap on Loopback0 from 4.4.4.4
*Jan 23 12:53:29.047: PIM(0): Received v2 Bootstrap on Serial0/1/1 from 10.0.4.2
*Jan 23 12:53:29.067: PIM(0): Received v2 Bootstrap on Serial0/1/0 from 10.0.3.2
*Jan 23 12:53:29.095: PIM(0): Update (224.0.0.0/4, RP:6.6.6.6), PIMv2
*Jan 23 12:53:29.095: PIM(0): Update (224.0.0.0/4, RP:4.4.4.4), PIMv2
*Jan 23 12:53:29.095: PIM(0): Update (224.0.0.0/4, RP:2.2.2.2), PIMv2
*Jan 23 12:53:29.095: PIM(0): Update (224.0.0.0/4, RP:5.5.5.5), PIMv2
*Jan 23 12:53:29.095: PIM(0): Update (224.0.0.0/4, RP:3.3.3.3), PIMv2
*Jan 23 12:53:29.095: PIM(0): Added with (224.0.0.0/4, RP:1.1.1.1), PIMv2
*Jan 23 12:53:29.039: PIM(0): Received v2 Bootstrap on Loopback0 from 4.4.4.4
*Jan 23 12:53:29.047: PIM(0): Received v2 Bootstrap on Serial0/1/1 from 10.0.4.2
*Jan 23 12:53:29.067: PIM(0): Received v2 Bootstrap on Serial0/1/0 from 10.0.3.2
*Jan 23 12:54:29.039: PIM(0): Update (224.0.0.0/4, RP:6.6.6.6), PIMv2
*Jan 23 12:54:29.039: PIM(0): Update (224.0.0.0/4, RP:4.4.4.4), PIMv2
*Jan 23 12:54:29.039: PIM(0): Update (224.0.0.0/4, RP:2.2.2.2), PIMv2
*Jan 23 12:54:29.039: PIM(0): Update (224.0.0.0/4, RP:5.5.5.5), PIMv2
*Jan 23 12:54:29.039: PIM(0): Update (224.0.0.0/4, RP:3.3.3.3), PIMv2
*Jan 23 12:54:29.039: PIM(0): Update (224.0.0.0/4, RP:1.1.1.1), PIMv2
```

Obr. 8.15: Výpis debugingu protokolu PIM zo smerovača Cisco

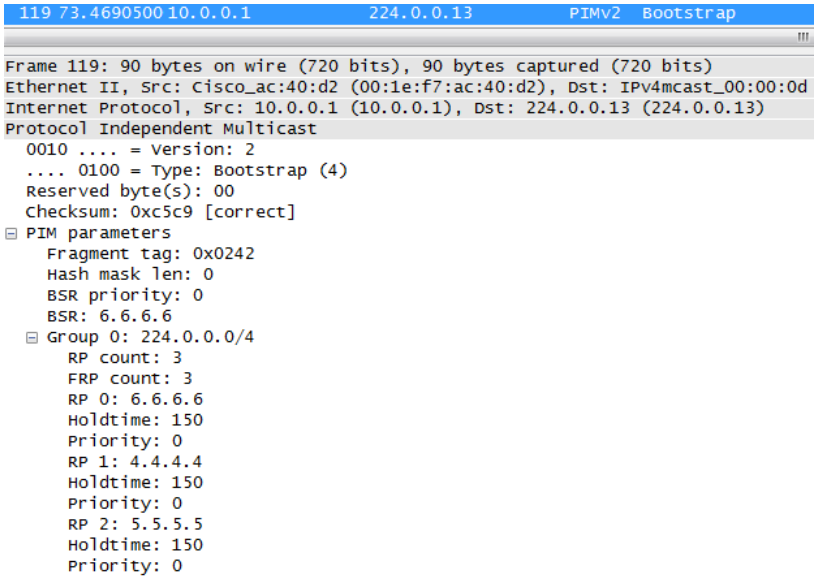
V debugu na smerovači Huawei (viď obr 8.16) sú výpisy obdobné, akurát je lepšie vidieť proces vyjednávania RP a určenie BSR pravdepodobne zostalo na smerovači Cisco, pretože na začiatku sa len aktivuje mechanizmus a už sa vyjednáva RP. Prípadne je tento proces lepšie viditeľný na informáciach ktoré niesu ľahko čitateľné. Na začiatku sa aktivuje BSR mechanizmus a pripraví sa odoslanie C-RP propagácie. Potom smerovač pošle kandidáta na RP s adresou 3.3.3.3 na adresu 6.6.6.6 (BSR). Ďalej vidíme, že správa obsahuje 1 prefix s nulovou prioritou. Po čase posiela znova propagácie BSR smerovaču.

Nakoniec prichádza správa od BSR smrovača v ktorej už je obsiahnutý zoznam kandidátov na RP.

```
Jan 28 2015 22:29:56.402.1-05:13 RAHuawei PIM/7/RP:(public net): Using BSR mechan
ism, Prepare to send C-RP-Adv (P19833)
Jan 28 2015 22:29:56.402.2-05:13 RAHuawei PIM/7/RP:(public net): PIM ver 2 C-RP s
ending 3.3.3.3 -> 6.6.6.6 on GigabitEthernet0/0/2 (S036841)
Jan 28 2015 22:29:56.402.3-05:13 RAHuawei PIM/7/RP:(public net): C-RP 3.3.3.3, pr
efix count 1, priority : 0, holdtime 150 (S036869)
:29:56.402.5-05:13 RAHuawei PIM/7/RP:(public net): Admin Scope Zone
: 0 (S036901)
Jan 28 2015 22:29:56.402.6-05:13 RAHuawei PIM/7/RP:(public net): Sent C-RP-Adv to
 BSR 6.6.6.6 (P191939)
Jan 28 2015 22:30:06.192.1-05:13 RAHuawei PIM/7/RP:(public net): PIM ver 2 BSR re
ceiving 10.0.0.1 -> 224.0.0.13 without N bit on GigabitEthernet0/0/2 (S036988)
Jan 28 2015 22:30:06.192.2-05:13 RAHuawei PIM/7/RP:(public net): BSR 6.6.6.6, fra
g 8688, pri 0, hash mask len 0 (S037011)
Jan 28 2015 22:30:06.192.3-05:13 RAHuawei PIM/7/RP:(public net): Group 224.0.0.0/
4: frags 6, C-RP's 6 (S037038)
Jan 28 2015 22:30:06.192.4-05:13 RAHuawei PIM/7/RP:(public net): 6.6.6.6 pri: 0,
holdtime: 150 (S037064)
Jan 28 2015 22:30:06.192.5-05:13 RAHuawei PIM/7/RP:(public net): 4.4.4.4 pri: 0,
holdtime: 150 (S037064)
Jan 28 2015 22:30:06.192.6-05:13 RAHuawei PIM/7/RP:(public net): 2.2.2.2 pri: 0,
holdtime: 150 (S037064)
Jan 28 2015 22:30:06.192.7-05:13 RAHuawei PIM/7/RP:(public net): 5.5.5.5 pri: 0,
holdtime: 150 (S037064)
Jan 28 2015 22:30:06.192.8-05:13 RAHuawei PIM/7/RP:(public net): 3.3.3.3 pri: 0,
holdtime: 150 (S037064)
Jan 28 2015 22:30:06.192.9-05:13 RAHuawei PIM/7/RP:(public net): 1.1.1.1 pri: 0,
holdtime: 150 (S037064)
```

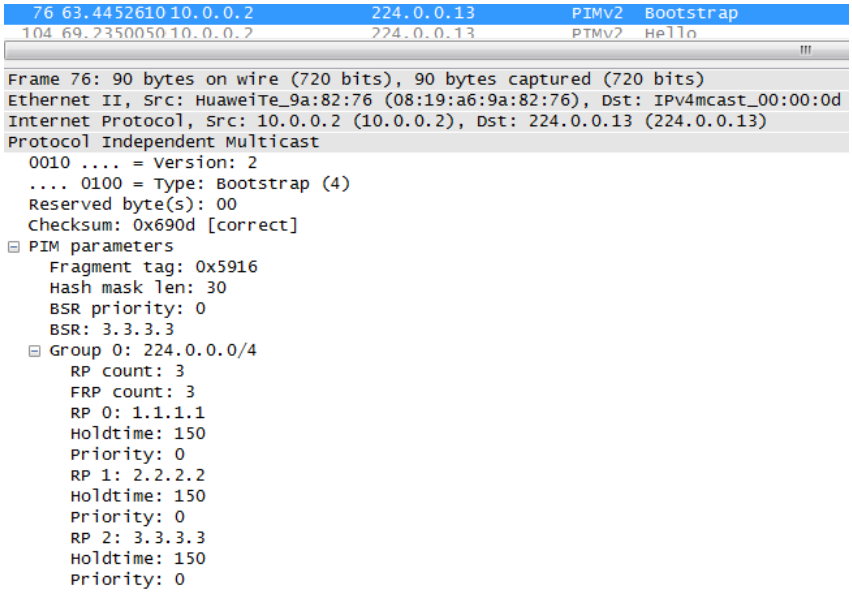
Obr. 8.16: Výpis debugingu protokolu PIM na smerovači Huawei

V záznamoch z komunikácie medzi RAHuawei a RACisco vidíme, ako v Bootstrap správach propagujú svoje BSR smerovače a kandidátov na RP. Na obrázku 8.17 vidíme, že RACisco ponúka ako BSR 6.6.6.6 a kandidáti na RP sú 6.6.6.6, 4.4.4.4 a 5.5.5.5.



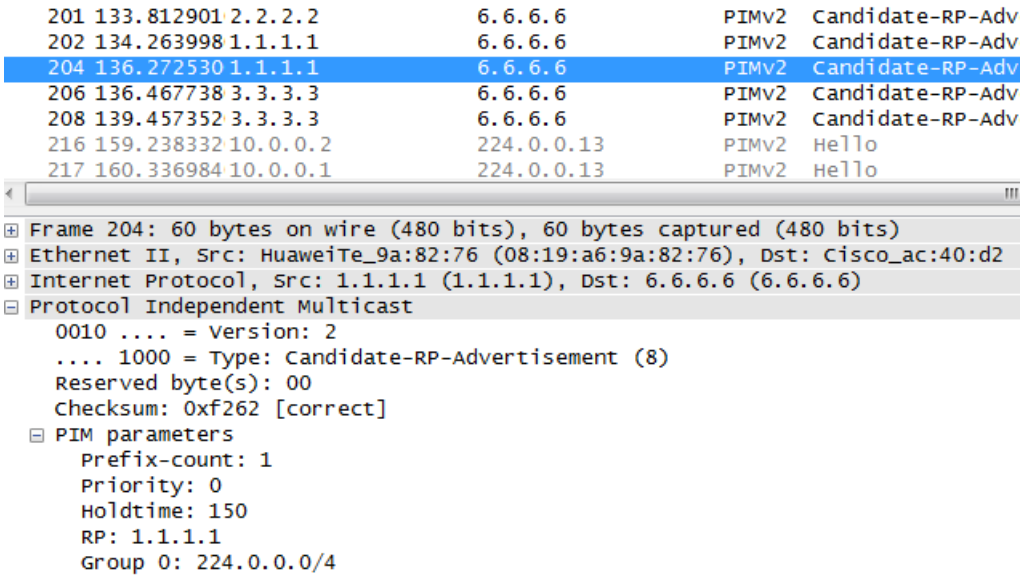

Obr. 8.17: Správa Boodstrap od smerovača RACisco

Smerovač RAHuawei zase ponúkal ako BSR smerovač s adresou 3.3.3.3 a kandidátmi na RP sú 1.1.1.1, 2.2.2.2 a 3.3.3.3. Ako BSR sa zvolí (vzhľadom ku konfigurácii) smerovač s vyššou IP a ten potom rozhoduje o RP.




Obr. 8.18: Správa Boodstrap od smerovača RAHuawei

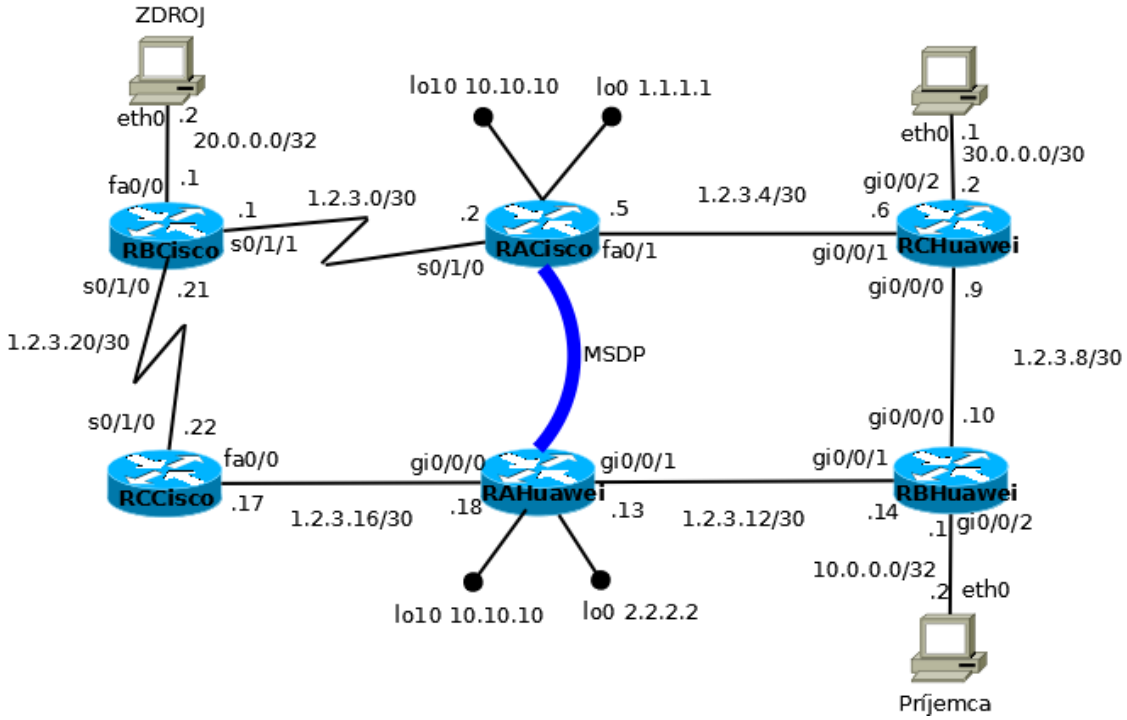
Ako BSR bol teda vybraný smerovač s IP 6.6.6.6 a ten teraz udržuje informácie o kandidátoch na RP a propaguje ich v sieti. Na obrázku 8.19 vidíme, že kandidáti na RP sa už nehlásia na adresu protokolu PIM (224.0.0.13) ale priamo BSR smerovaču.




Obr. 8.19: Správa Boodstrap od smerovača RAHuawei

## 8.5 Nastavenie pre Anycast RP

Pri tejto konfigurácii som vychádzal zo schémy na obrázku 8.20. Anycast RP v podstate rozširuje možnosti protokolu PIM-SM využívajúc protokolu MSDP. Preto je nutné na všetkých smerovačoch nastaviť Protokol PIM-SM (so statickým RP) a na smerovačoch, ktoré majú zdielať medzi sebou informácie MSDP. Nastavovaniu protokolu PIM sa v tejto kapitole nebudem opätovne venovať a popíšem len nastavenie MSDP väzby.




Obr. 8.20: Topológia siete pre PIM SM Anycast RP

Smerovač od firmy Cisco sa konfiguruje:

- Nastavenie spojenia s peerom
  - *Router(config)#ip msdp peer <ip addresa peera> connect-source <rozhranie>*
- Nastavenie pôvodcu spojenia
  - *Router(config)#ip msdp originator-id <rozhranie>*

Na smerovači Huawei bola konfigurácia nasledovná:

- Vstuo do konfigurácie MSDP
  - *[Router]msdp*
- Nastavenie pôvodcu msdp
  - *[Router-msdp]originating-rp <rozhranie>*
- Nastavenie spojenia s peerom

– *[Router-msdp]peer <ip adresa peera> connect-interface <rozhrnie>*

Aby Anycast RP fungovalo správne, je nutné nastaviť na smerovačoch, ktoré sú prepojené MSDP väzbou loopback rozhrania s rovnakými IP adresami. Rovnakú adresu potom použiť na ostatných (nie peerujúcich smerovačoch) ako statický RP. Tak ako je to vidieť v konfiguráciách smerovačov v prílohe G (Prílohy).

## 8.6 Overenie funkčnosti Anycast RP

Táto konfigurácia funguje, MSDP väzbu sa smerovačom podarilo nadviazať. O tom svedčí výpis zo smerovača Cisco na obrázku 8.21 a smerovača Huawei na obrázku 8.22. Na výpisoch sú podobné informácie akurát z opačných strán spojenia.

```
sh ip msdp peer
MSDP Peer 2.2.2.2 (?), AS ?
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (1.1.1.1)
    Uptime(Downtime): 00:07:22, Messages sent/received: 8/10
    Output messages discarded: 0
    Connection and counters cleared 00:10:00 ago
    Elapsed time since last message: 00:00:17
    Local Address of connection: 1.1.1.1
    Local Port: 30564, Remote Port: 639
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 1
    Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
  Message counters:
    RPF Failure count: 0
    SA Messages in/out: 5/0
    SA Requests in: 0
    SA Responses out: 0
    Data Packets in/out: 0/0
```

Obr. 8.21: Výpis nastavení MSDP zo smerovača Cisco

Na výpise zo smerovača Cisco vidíme, že väzba je nadviazaná na adresu 2.2.2.2 z adresy 1.1.1.1, ktorá prislúcha k rozhraniu Loopback0. Status spojenia je Up. Z teoretickej časti vieme, že MSDP komunikuje na porte 639 čo dokazuje aj tento výpis, a ako lokálny port bol zvolený 30564.

```
disp msdp peer-status
MSDP Peer Information of VPN-Instance: public net
  MSDP Peer 1.1.1.1, AS ?
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:08:08
    Resets: 1
    Connection interface: LoopBack0 (2.2.2.2)
    Number of sent/received messages: 17/10
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:11:38
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/6
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
  Peer authentication: unconfigured
  Peer authentication type: none
```

Obr. 8.22: Výpis nastavení MSDP zo smerovača Huawei

Výpis zo smerovača Huawei obsahuje v základe rovnaké informácie, akurát je chudobnejší o informácie aké porty sú použité. Na overenie funkčnosti existujú aj iné kontrolné výpisy ako u Huaweiu tak u Cisca, ale tie neobsahujú viac informácii než výpisy, ktoré sú už uvedené. Obsahujú len adresu peera, status spojenia a dobu po ktorú je MSDP spojenie nadviazané. Preto pre overenie správnosti konfigurácie nazrieme do debugov na oboch smerovačoch.

Na začiatku debugu (obr. 8.23) vidíme, že smerovač posiela TCP connect smerom k možnému peerovi. Ten zo spojením súhlasí, takže spojenie dostáva stav Up. Spojenie je nadviazané a môžu si vymieňať správy. Vo výpise vidíme aj, že smerovač dostáva a odosiela Keepalive správy. Vo štvrtom riadku z dola vidíme správu, ktorá informuje o existujúcom zdroji multicastu pre skupinu 239.255.0.10 s adresou 20.0.0.2. Smerovač má príjemcu pre danú skupinu, preto si túto informáciu prevezme a rozšíri distribučný strom.

```
*Jan 29 14:54:46.483: MSDP(0): 2.2.2.2: Sending TCP connect
*Jan 29 14:54:46.495: MSDP-5-PEER_UPDOWN: Session to peer 2.2.2.2 going up
*Jan 29 14:54:46.495: MSDP(0): 2.2.2.2: TCP connection established
*Jan 29 14:54:46.499: MSDP(0): 2.2.2.2: Keepalive TLV
*Jan 29 14:54:46.663: MSDP(0): 2.2.2.2: Sending Keepalive message to peer
*Jan 29 14:54:47.459: MSDP(0): 2.2.2.2: SA TLV, len: 20, ec: 1, RP: 2.2.2.2
*Jan 29 14:54:47.459: MSDP(0): 2.2.2.2: Peer RPF check passed for single peer
*Jan 29 14:54:47.459: MSDP(0): (20.0.0.2/32, 239.255.0.10), accepted
*Jan 29 14:54:47.459: MSDP(0): WAVL Insert SA Source 20.0.0.2 Group 239.255.0.10 RP 2.2.2.2
    Successful
*Jan 29 14:54:47.663: MSDP(0): 2.2.2.2: Originating SA message, originator-id 1.1.1.1
*Jan 29 14:54:47.663: MSDP(0): 2.2.2.2: Building SA message from SA cache
```

Obr. 8.23: Výpis debugingu protokolu MSDP na smerovači Cisco

V debugu zo smerovača Huawei (obr. 8.24) vidíme proces z opačnej strany. Na začiatku načúva na TCP či sa neobjaví nejaký možný peer. V d'alšom riadku súhlasí s vytvorením spojenia. Spojenie je nadviazané a posiela peerovi Keepalive správu. Na konci výpisu vidíme, že pridáva záznam o zdroji pre skupinu do SA (Source Active) správy a odosiela túto správu peerovi.

```
Jan 29 2015 23:04:33.960.1+00:00 1220 MSDP/7/CONNECT:
(public net): 1.1.1.1: TCP listening(13) (H121063)
Jan 29 2015 23:05:03.590.2+00:00 1220 MSDP/7/CONNECT:
(public net): 1.1.1.1: Connection accepted(14) (H121209)
Jan 29 2015 23:05:03.590.3+00:00 1220 MSDP/7/CONNECT:
(public net): 1.1.1.1: TCP connection established (H121213)
Jan 29 2015 23:05:03.590.4+00:00 1220 MSDP/7/EVENT:
(public net): 1.1.1.1: Sending message to peer: keepalive (H101097)
Jan 29 2015 23:05:03.590.5+00:00 1220 MSDP/7/EVENT:
(public net): 1.1.1.1: Originating SA message for peer (H10900)
Jan 29 2015 23:05:04.550.1+00:00 1220 MSDP/7/EVENT:
(public net): Adding (20.0.0.2, 239.255.0.10) entry into SA message (H10501)
```

Obr. 8.24: Výpis debugingu protokolu MSDP na smerovači Huawei

# 9 Konfigurácia PIMv6

Tento protokol (známy aj ako IPv6 PIM) je v podstate ekvivalentom protokolu PIM . V práci ho uvádzam samostatne pre lepšiu orientáciu. Jeho princíp činnosti zostáva nezmenený, menia sa len adresy s ktorými pracuje.

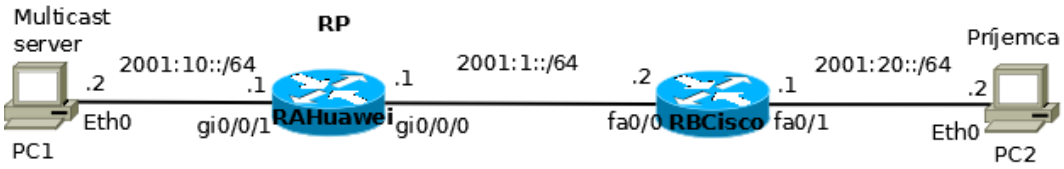
Za účelom použitia tohto protokolu bol nutný upgrade na smerovači Huawei, pretože firmware s ktorým bolo zariadenie dodané nepozná IPv6 multicast, ako som už spomínal v kapitole MLD Snooping.

Testovať sa bude PIMv6 len pre riedky režim (sparse mode), pretože spoločnosť Cisco nemá implementáciu pre hustý režim (dense mode). U smerovača Huawei je možné Dense Mode aktivovať, no nakoľko bol vylepšený firmware len na jednom, je ťažké posúdiť či funguje správne alebo nie.

Preto podobne ako u IPv4 verzie, je nutné zabezpečiť unicastové smerovanie. Ja som za týmto účelom používal OSPFv3.

## 9.1 Nastavenia smerovačov

Táto konfigurácia sa oproti klasickému PIM-SM líši v podstate len adresami a tým, že na prihlasovanie do skupín sa používa MLD. Táto konfigurácia využíva statické určenie RP. Avšak aplikovateľný je aj spôsob z PIMu pre IPv4 s využitím BSR. Zapojenie vychádza z topológie na obrázku 9.1.




Obr. 9.1: Topológia siete pre PIMv6

Konfigurácia smerovača Cisco je nasledovná:

- Povolenie multicastoveho smerovania
  - *Router(config)# ipv6 multicast-routing*
- Na rozhraní, na ktorom chceme povoliť protokol PIM SM
  - *Router(config-if)# ipv6 pim*

- Nastavenie statickej adresy RP
  - *Router(config)# ipv6 pim rp-address <adresa RP>*

Konfigurácia smerovača RBCisco je v prílohe H.2 (Prílohy).
Na smerovači Huawei je konfigurácia nasledovná:

- Povolenie multicastoveho smerovania
  - *[Router]multicast ipv6 routing-enable*
- Na rozhraní, na ktorom chceme povoliť protokol PIM SM
  - *[Router-GigabitEthernet0/0/0]pim ipv6 sm*
- Na rozhraní vedúcom k užívateľskej stanici (alebo multicast servru)
  - *[Router-GigabitEthernet0/0/1]mld enable*
- Nastavenie statickej adresy RP
  - *[Router]pim-ipv6*
  - *[Router-pim]static-rp <adresa RP>*

Konfigurácia smerovača RAHuawei je v prílohe H.1 (Prílohy).

## 9.2 Overenie funkčnosti konfigurácie

Táto konfigurácia funguje bez problémov pokiaľ neberiem v úvahu, že bolo kvôli tejto funkcionalite nutné meniť firmware.

Na obrázkoch 9.3 a 9.2 vidíme, že smerovače správne zostavili multicastove smerovacie tabuľky. Z Výpisu smerovača Cisco je zjavné, že vysielanie pre skupinu FF05::1::4 prichádza z rozhrania Fa0/0. Rendevouz point má adresu 2001:1::1. Adredsa zdroja pre spomínanú multicastovú skupinu je 2001:10::2. A spracovaný multicast opúšťa smerovač rozhraním Fa0/1.

```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, FF05::1:4), 00:04:55/never, RP 2001:1::1, flags: SCJ
  Incoming interface: FastEthernet0/0
  RPF nbr: FE80::A19:A6FF:FE9B:6D4E
  Immediate Outgoing interface list:
    FastEthernet0/1, Forward, 00:04:55/never

(2001:10::2, FF05::1:4), 00:03:15/00:00:14, flags: SJT
  Incoming interface: FastEthernet0/0
  RPF nbr: FE80::A19:A6FF:FE9B:6D4E
  Inherited Outgoing interface list:
    FastEthernet0/1, Forward, 00:04:55/never
```

Obr. 9.2: Výpis multicastovej smerovacej tabuľky smerovača Cisco

Na výpise so smerovača Huawei vidíme totožné informácie. Doplnené o informácie, že sa jedná o PIM-SM a adresa RP patrí lokálnemu rozhraniu.

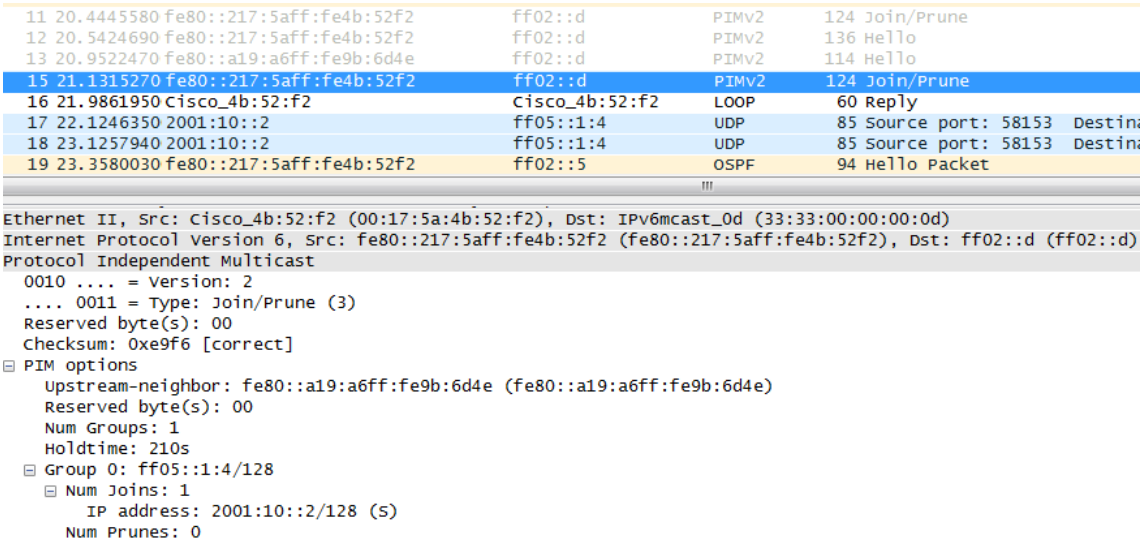
```
display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FF05::1:4)
     RP: 2001:1::1 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:01:58
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/0
             Protocol: pim-sm, UpTime: 00:01:58, Expires: 00:03:29

 (2001:10::2, FF05::1:4)
     RP: 2001:1::1 (local)
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 00:03:43
     Upstream interface: GigabitEthernet0/0/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/0
             Protocol: pim-sm, UpTime: 00:01:58, Expires: 00:03:29
```

Obr. 9.3: Výpis multicastovej smerovacej tabuľky smerovača Cisco

V zázname z komunikácie medzi smerovačmi (Obr. 9.4) vidíme, že pri nasadení IPv6 PIM sa aj signalizačné správy (PIMv2) preorientujú na IPV6. V zvýraznenom riadku napríklad vidíme správu Join/Prune od smerovača Cisco. Touto správou žiada RP (smerovač Huawei) o priradenie do skupiny ff05::1:4 so zdrojom 2001:10::2. Po priradení do skupiny začali prechádzať UDP pakety (generované scriptom v pythone), ktoré predstavujú multicastové data.




Obr. 9.4: Záznam komunikácie medzi RAHuawei a RBCisco

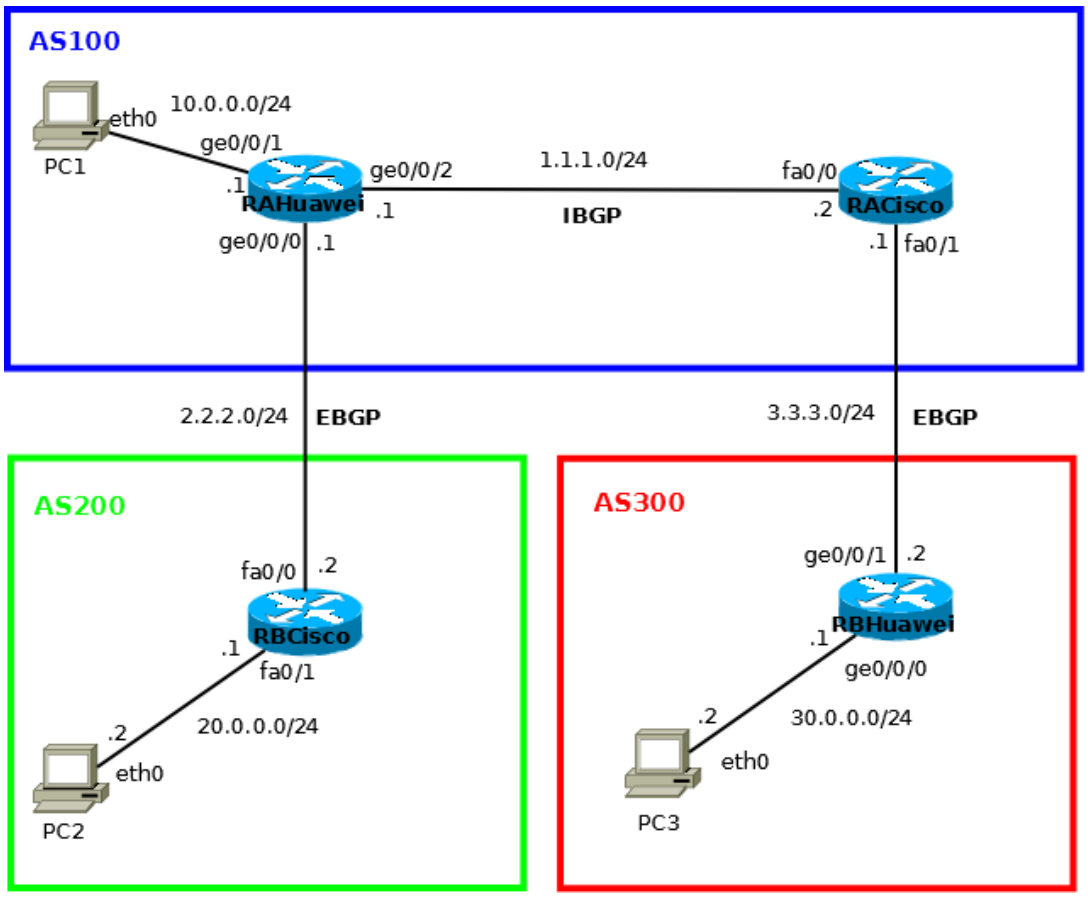
# 10 Konfigurácia MBGP

Pre správne fungovanie MBGP je nutné zabezpečiť funkcionalitu BGP. Pri konfigurácii som zostavil tri AS (Autonomne Systémy), aby sa dali vysledovať správy pri eBGP aj iBGP. Pri MBGP je vlastne výsledkom práce, že sa v podstate automaticky vybudujú statické cesty.

To znamená, že v jednotlivých AS funguje klasický protocol PIM a v prípade, že by multicast bolo nutné rozosielať mimo AS sa o to postará MBGP.

## 10.1 Nastavenie smerovačov

Smerovače boli zapojené podla topológie na obrázku 10.1.




Obr. 10.1: Topológia siete pre MBGP

Pri tejto konfigurácii je nutné najskôr dosiahnuť funkčné unicast smerovanie (ktoré nebudem popisovať) a funkčné nastavenie protokolu PIM (doporučený je PIM-SM), ktoré som popisoval v predchádzajúcich kapitolách.

Po dodržaní týchto krokov stačí smerovačom nastaviť možnosť prenášať rodinu adries IPv4 multicast. Konfigurácia smerovača Cisco je nasledovná:

- Vstup do nastavení smerovacieho protokolu BGP
  - *Router(config)# router bgp <číslo as>*
- Vstup do nastavení rodiny adries ipv4 multicast
  - *Router(config-router)# address-family ipv4 multicast*
- Aktivovanie prenosu multicastu na danú adresu.
  - *Router(config-router-af)# neighbor <adresa> activate*
- Možnosť pridania suseda pridaním siete
  - *Router(config-router-af))# network <adresa> mask <maska>*

Konfigurácie smerovačov sú v prílohách I.3 a I.4 (Prílohy).

Na smerovači Huawei je konfigurácia nasledovná:

- Vstup do nastavení smerovacieho protokolu BGP
  - *[Router]bgp <číslo AS>*
- Vstup do nastavení rodiny adries ipv4 multicast
  - *[Router-bgp] ipv4-family multicast*
- Aktivovanie prenosu multicastu na danú adresu.
  - *[Router-bgp-af-multicast]peer <adresa> enable*
- Možnosť pridania statických ciest
  - *[Router-bgp-af-multicast]import-route static*

Konfigurácie smerovačov sú v prílohách I.1 a I.2 (Prílohy).

## 10.2 Overenie funkčnosti konfigurácie

Táto konfigurácia fungovala napriek menším nejasnostiam. MBGP zostavilo na všetkých smerovačoch multicastove smerovacie tabuľky. Príklad tejto tabuľky zo smerovača Huawei vidíme na obrázku 10.2 a zo smerovača Cisco na obrázku 10.3.

```
[RAHuawei]dis bgp multicast routing-table

 BGP Local router ID is 10.0.0.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 11
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.0/24         0.0.0.0         0                    0      ?
 *>   1.1.1.1/32         0.0.0.0         0                    0      ?
 *>   2.2.2.0/24         0.0.0.0         0                    0      ?
 *>   2.2.2.1/32         0.0.0.0         0                    0      ?
 *>i  3.3.3.0/24         1.1.1.2         0          100       0      300?
 *>   10.0.0.0/24        0.0.0.0         0                    0      ?
 *>   10.0.0.1/32        0.0.0.0         0                    0      ?
 *>   20.0.0.0/24        2.2.2.2         0                    0      200i
 *>i  30.0.0.0/24        1.1.1.2         0          100       0      300?
 *>   127.0.0.0          0.0.0.0         0                    0      ?
 *>   127.0.0.1/32       0.0.0.0         0                    0      ?
```

Obr. 10.2: Multicastová smerovacia tabuľka smerovača RAHuawei

```
RBCisco#sh ip bgp ipv4 multicast
BGP table version is 17, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.0/24       2.2.2.1                  0             0 100 ?
*> 2.2.2.0/24       2.2.2.1                  0             0 100 ?
*> 3.3.3.0/24       2.2.2.1                                0 100 300 ?
*> 10.0.0.0/24      2.2.2.1                  0             0 100 ?
*> 20.0.0.0/24      0.0.0.0                  0         32768 i
*> 30.0.0.0/24      2.2.2.1                                0 100 300 ?
```

Obr. 10.3: Multicastová smerovacia tabuľka smerovača RBcisco

Z obrázkov vidíme, že smerovače nevedia pri externých trasách identifikovať typ spojenia. Pri záznamoch (ktoré sú vzhladom k topoogii všetky správne) sa na konci uvádza kód pôvodu. Záznamy prameniace z internej väzby (IGP) majú správne určené písmeno i (podľa vysvetliviek na obrázkoch) no ostatné záznamy majú otázniky. Podobne vyzerajú výpisy MBGP smerovacích tabuliek aj z ostatných smerovačov.

Tento detail však nemal žiadny dopad na komunikáciu. Multicastové dáta prechádzali bez problémov jednotlivými AS až na miesto doručenia. Jednotlivé smerovače dokázali identifikovať svojich peerov a komunikovať s nimi, čo ukazujú obrázky 10.4 a 10.5.

```
[RBHUawei]display bgp multicast peer

 BGP local router ID : 3.3.3.2
 Local AS number : 300
 Total number of peers : 1                 Peers in established state : 1

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Prv

  3.3.3.1         4         100       26       23     0 00:17:58 Established   4
```

Obr. 10.4: Informácie o peeroch na smerovači RBHuawei

Smerovač RBHuawei má adresu 3.3.3.2 (zvolil si ju ako ID) a jeho peer adresu 3.3.3.1. Vidíme, že status komunikácie je Established (nadviazaný) a smerovače medzi sebou komunikujú, pretože si vymieňajú správy (MsgRcvd a Msg Sent).

```
RACisco#sh ip bgp ipv4 multicast summary
BGP router identifier 3.3.3.1, local AS number 100
BGP table version is 13, main routing table version 13
6 network entries using 702 bytes of memory
6 path entries using 288 bytes of memory
5/3 BGP path/bestpath attribute entries using 620 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1658 total bytes of memory
BGP activity 35/22 prefixes, 51/38 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.1.1.1         4   100     124     139       13    0    0 00:57:55        4
3.3.3.2         4   300     103     119       13    0    0 00:29:59        2
```

Obr. 10.5: Informácie o susedoch na smerovači RACisco

Podobné informácie vidíme aj na smerovači RACisco. Z výpisu vidíme, že tento smerovač je susedný so smerovačom RBHuawei. Jeho adresa je 3.3.3.1 a adresa jedneho jeho peera 3.3.3.2 (RBHuawei), druhým peerom je smerovač s adresou 1.1.1.1 (RAHuawei). Spojenia sú nadviazané a komunikácia stále prebieha, čo vidíme na zvýšených hodnotách MsgRcvd a MsgSent.

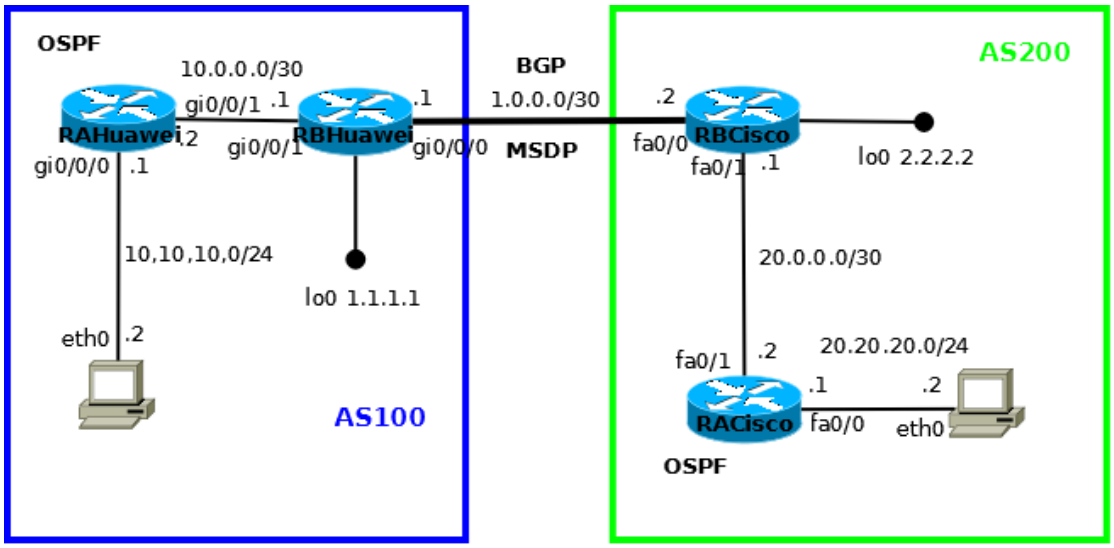
# 11 Konfigurácia MSDP

Pre správne fungovanie MSDP je nutné, aby v topológii bolo funkčné klasické unicastové smerovanie, funkčný protokol BGP a nastavený protokol PIM. Týmto jednotlivým nastaveniam sa už venovať nebudem, pretože sú popísané v prechádzajúcich kapitolách.

Protokol MSDP som už síce taktiež spomínal pri Anycast RP, ale to bolo v rámci doručovania multicastu vnútri domény. Táto konfigurácia je na prepájanie domén a teda to na čo bol protokol MSDP navrhnutý.

## 11.1 Nastavenia smerovačov

Táto sieť bola zapojená podľa obrázka 11.1. Každý AS funguje ako samostatná doména smerovaná na základe protokolu OSPF. Tieto domény sú prepojene protokolom BGP a zdieľajú svoje RP informácie prostredníctvom MSDP.




Obr. 11.1: Topológia pre MSDP

Konfigurácia MSDP je veľmi jednoduchá. Zložité sú všetky konfigurácie, ktoré následnému spusteniu MSDP predchádzajú. Konfigurácia na smerovači Cisco bola nasledovná:

- Nastavenie spojenia s peerom
  - *Router(config)#ip msdp peer <ip addresa peera> connect-source <rozhranie>*

A na smerovači Huawei nasledovná:

- Vstup do konfigurácie MSDP
  - *[Router]msdp*
- Nastavenie spojenia s peerom
  - *[Router-msdp]peer <ip adresa peera> connect-interface <rozhrnie>*

Presné konfigurácie jednotlivých smerovačov sú v prílohách J.4, J.3 pre Cisco a v prílohách J.1 a J.2 (Prílohy) pre smerovače Huawei.

## 11.2 Overenie funkčnosti konfigurácie

Toto zapojenie fungovalo správne. MSDP väzba bola nadviazaná a smerovače si predávajú informácie. Na obrázkoch 11.2 a 11.3 vidíme veľmi podobné výpisy zo smerovačov prepojených pomocou MSDP.

```
[RBHuawei]dis msdp peer-status
MSDP Peer Information of VPN-Instance: public net
  MSDP Peer 1.0.0.2, AS 200
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:05:52
    Resets: 0
    Connection interface: GigabitEthernet0/0/0 (1.0.0.1)
    Number of sent/received messages: 13/17
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:16:21
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 2, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 13/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 3/0
  Peer authentication: unconfigured
  Peer authentication type: none
```

Obr. 11.2: Informácie o MSDP peeroch na smerovači RBHuawei

Prvý riadok oboch výpisov obsahuje informácie o adrese MSDP peera. Vidíme, že MSDP prebralo informácie z protokolu BGP a identifikovalo, v ktorom AS sa daný peer nachádza. Ďalej je z výpisov čitateľný status, ktorý je up a zdroj pripojenia.

```
RBCisco#sh ip msdp peer
MSDP Peer 1.0.0.1 (?), AS 100
  Connection status:
    State: Up, Resets: 1, Connection source: FastEthernet0/0 (1.0.0.2)
    Uptime(Downtime): 00:06:24, Messages sent/received: 11/7
    Output messages discarded: 0
    Connection and counters cleared 00:10:22 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 0
    Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
  Message counters:
    RPF Failure count: 0
    SA Messages in/out: 0/6
    SA Requests in: 0
    SA Responses out: 0
    Data Packets in/out: 0/2
```

Obr. 11.3: Informácie o MSDP peeroch na smerovači RBCisco

Hlavný rozdiel pri prepájaní AS pomocou MSDP voči jeho vnútro doménovému použitiu je, že nemusia byť všade nastavené statické RP, ale smerovače si môžu voliť RP automaticky prostredníctvom BSR. Na výpisoch z multicastových smerovacích tabuliek obrázky11.4 a 11.5 vidíme, že pre skupinu 239.255.0.10 bol zvolený RP s adresou 2.2.2.2. Tieto výpisy znova dokazujú, že táto konfigurácia je funkčná, pretože zo záznamov vidíme, že distribučný strom je vytvorený skrz AS.

Pre upresnenie rozpíšem. Napríklad smerovač RBHuawei patrí do AS 100, v ktorom je zdroj multicastu s adresou 10.10.10.2. O tomto zdroji sa dozvedel štandardne z protokolu PIM. Túto informáciu zabalil a prostredníctvom MSDP poslal susedovi, čo dokazuje záznam v tabuľke smerovača RBCisco, ktorý je situovaný v AS200.

```
[RBHuawei]disp pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 2 (S, G) entries

 (10.10.10.2, 239.255.0.10)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:03:35
     Upstream interface: GigabitEthernet0/0/1
         Upstream neighbor: 10.0.0.2
         RPF prime neighbor: 10.0.0.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/0
             Protocol: pim-sm, UpTime: 00:03:35, Expires: 00:02:52

 (20.20.20.2, 239.255.0.10)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: ACT
     UpTime: 00:04:42
     Upstream interface: GigabitEthernet0/0/0
         Upstream neighbor: 1.0.0.2
         RPF prime neighbor: 1.0.0.2
     Downstream interface(s) information: None
```

Obr. 11.4: Multicastova smerovacia tabuľka RBHuawei

```
RBCisco#show ip mr
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.0.10), 00:03:05/00:03:20, RP 2.2.2.2, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:01:53/00:03:20

(10.10.10.2, 239.255.0.10), 00:01:45/00:03:20, flags: TA
  Incoming interface: FastEthernet0/0, RPF nbr 1.0.0.1
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:01:45/00:03:20

(20.20.20.2, 239.255.0.10), 00:03:05/00:01:40, flags: PT
  Incoming interface: FastEthernet0/1, RPF nbr 20.0.0.2
  Outgoing interface list: Null

(*, 224.0.1.40), 00:55:11/00:02:20, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Loopback0, Forward/Sparse, 00:55:11/00:02:20
```

Obr. 11.5: Multicastová smerovacia tabuľka RBCisco

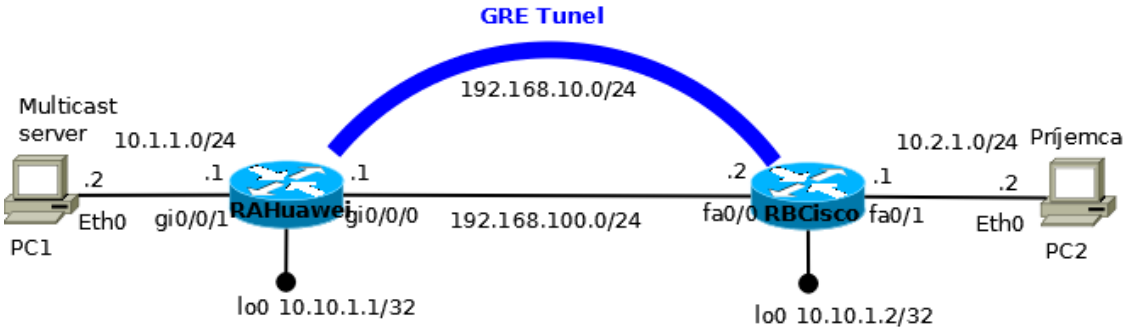
# 12 Konfigurácia Multicast over GRE

Zaujímavým spôsobom ako dostať multicastove vysielanie skrz cudzí autonómny systém je použitie tunelu. Táto konfigurácia vychádza z aplikovania protokolu PIM na rozhranie Tunelu.

Pre úplnosť rôznych aplikácii je vhodné ukázať aj spôsob, ktorým môže zostať fyzické rozhranie nedotknuté a vytvoríme virtuálne rozhranie (tunel), ktoré bude rozširovať distribučný strom za hranice AS bez nutnosti konfigurácie siete ktorou prechádza.

## 12.1 Nastavenia Smerovačov

Topológia bola zapojená podľa obrázka 12.1. V obrázku je síce naznačený zdroj multicastu za smerovačom Huaweei, no pri testovaní vždy skúšam všetky možnosti. Pre správny beh je nutné nastaviť unicastové smerovanie, ktorému sa venovať nebudem. Zostavenie tunelu a nastavenie protokolu PIM popíšem v tejto kapitole.




Obr. 12.1: Topológia siete pre Multicast over GRE

Konfigurácia smerovača Cisco je nasledovná:

- Vstup na rozhranie tunelu
  - *Router(config)#int tun <číslo>*
- Nastavenie adresy tunelu
  - *Router(config-if)#ip add <adresa> <maska>*
- Povolenie protokolu PIM-sm
  - *Router(config-if)#ip pim sparse-mode>*

- Nastavenie zdroju tunela
  - *Router(config-if)#tunnel source <rozhranie>*
- Nastavenie cieľu tunela
  - *Router(config-if)#tunnel destination <adresa>*
- Vrátiť sa o úroveň vyššie
  - *Router(config-if)#exit*
- Nastaviť rozhranie tunelu ako BSR kandidáta
  - *Router(config)#ip pim bsr-candidate Tunnel<číslo>*
- Nastaviť rozhranie tunelu ako RP kandidáta
  - *Router(config)#ip pim rp-candidate Tunnel<číslo>*

Konfigurácia smerovača Huawei:

- Vytvorenie rozhrania tunel
  - *[Router]int tunnel<číslo>*
- Nastavenie IP adresy tunelu
  - *[Router-Tunnel0/0/1]ip addres <adresa> <maska>*
- Nastavenie typu tunelovacieho protokolu
  - *[Router-Tunnel0/0/1]tunnel-protocol gre*
- Nastavenie zdroja tunelu
  - *[Router-Tunnel0/0/1]source <rozhranie>*
- Nastavenie cieľa tunelu
  - *[Router-Tunnel0/0/1]destination <adresa>*
- Povolenie protokolu PIM-SM na tomto rozhraní

  - *[Router-Tunnel0/0/1]pim sm*

- Vystúpenie o úroveň vyššie
  - *[Router-Tunnel0/0/1]quit*
- Výstup ku konfigurácii PIM
  - *[Router]pim*
- Nastavenie tunelu ako BSR kandidáta
  - *[Router-pim]c-bsr tunnel<číslo>*
- Nastavenie tunelu ako RP kandidáta
  - *[Router-pim]c-rp tunnel<číslo>*

Skrátené konfigurácie sa nachádzajú v prílohe K (Prílohy).

## 12.2 Overenie konfigurácie

Táto konfigurácia napriek svojej jednoduchosti a výpisom, ktoré budia dojem, že všetko funguje ako má nie je celkom funkčná. Na obrázku 12.2 a obrázku 12.3 vidíme výpisy PIM rozhraní z oboch smerovačov. To dokazuje, že smerovač môže aktivovať protokol PIM pre tunelové rozhranie.

```
[RAHuawei]display pim  interface
 VPN-Instance: public net
 Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
 GE0/0/1             up    0      30         1          10.1.1.1        (local)
 Tun0/0/1            up    1      30         1          192.168.10.2
```

Obr. 12.2: Výpis rozhraní PIM na smerovači RAHuawei

```
RBCisco#sh ip pim interface

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
10.2.1.1         FastEthernet0/1          v2/S   0      30     1      10.2.1.1
192.168.10.2     Tunnel0                  v2/S   1      30     1      0.0.0.0
```

Obr. 12.3: Výpis rozhraní PIM na smerovači RBCisco

Na výpise zo smerovacej tabuľky (obr. 12.4) vidíme, že cesty sa bez problémov vybudovali. Ako upstream rozhranie figuruje práve nami nastavený Tunnel0/0/1. Na tomto výpise už je vidieť aj problém, ktorý sa vyskytol. Druhý záznam tabuľky patrí zdroju, ktorý je umiestnený za smerovačom Cisco (na druhej strane tunela). Toto spojenie prebieha bez problémov. Problém je s komunikáciou, ktorej patrí posledný záznam. Tento zdroj je umiestnený na priamo pripojenom rozhraní Gi0/0/1 a jeho vysielanie nieje doručované do cieľa.

```
disp pim routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 2 (S, G) entries

 (*, 239.0.0.1)
     RP: 192.168.10.2
     Protocol: pim-sm, Flag: WC
     UpTime: 00:00:12
     Upstream interface: Tunnel0/0/1
         Upstream neighbor: 192.168.10.2
         RPF prime neighbor: 192.168.10.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/1
             Protocol: igmp, UpTime: 00:00:12, Expires: -

 (10.2.1.2, 239.0.0.1)
     RP: 192.168.10.2
     Protocol: pim-sm, Flag: ACT
     UpTime: 00:00:12
     Upstream interface: Tunnel0/0/1
         Upstream neighbor: 192.168.10.2
         RPF prime neighbor: 192.168.10.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/1
             Protocol: pim-sm, UpTime: 00:00:12, Expires: -

 (10.1.1.2, 239.255.0.10)
     RP: 192.168.10.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 00:03:38
     Upstream interface: GigabitEthernet0/0/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information: None
```

Obr. 12.4: Multicastová smerovacia tabuľka na smerovači RAHuawei

Keď sa pozrieme do multicastovej tabuľky smerovača Cisco (obr. 12.5), nevidíme žiadny záznam, ktorý by patril zdroju s adresou 10.1.1.2. Všetky ostatné záznamy sú v poriadku a korešpondujú s výpisom zo smerovača Huawei.

```
sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.0.0.1), 00:07:33/00:02:53, RP 192.168.10.2, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:00:36/00:02:53

(10.2.1.2, 239.0.0.1), 00:00:52/00:03:25, flags: T
  Incoming interface: FastEthernet0/1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:00:36/00:02:53

(*, 224.0.1.40), 01:31:54/00:02:16, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 01:31:49/00:02:16
```

Obr. 12.5: Multicastová smerovacia tabuľka na smerovači RBCisco

Z predošlých informácii by sa zdalo, že multicastove vysielanie zdroja 10.1.1.2 neopustí smerovač RAHuawei. V debugu na smerovači Huawei vyzeral priebeh komunikácie v poriadku. Neboli vypísané žiadne chybové hlásenia. Naproti tomu na smerovači Cisco sa objavilo hlásenie, ktoré je zobrazené na obrázku 12.6. V tomto hlásení vidíme, že z tunelu prišla žiadosť o zaregistrovanie zdroja 10.1.1.2 pre skupinu 239.255.0.10. Smerovač sa pokúsil overiť spätnú cestu k tomuto cieľu a toto testovanie neprešlo. Preto bolo zaregistrovanie zdroja odmietnuté. A multicastové dáta nemohli byť doručené príjamjúcej stanici. Tento problém beriem ako nezhodnu medzi zariadeniami Cisco a Huawei nakoľko vzhladom ku konfigurácii by tento problem nemal nastať.

```
*Apr  8 13:45:28.459: PIM(0): Received v2 Register on Tunnel0 from 10.1.1.1
*Apr  8 13:45:28.459:      for 10.1.1.2, group 239.255.0.10
*Apr  8 13:45:28.459: PIM(0): RPF lookup failed to source 10.1.1.2
*Apr  8 13:45:28.459: PIM(0): Send v2 Register-Stop to 10.1.1.1 for 10.1.1.2,
                      group 239.255.0.10
```

Obr. 12.6: Hlásenie z debugu smerovača RBCisco

# 13 Porovnanie zariadení Cisco a Huawei

Počas testovania navrhnutých topológii sa zariadenia prejavovali rôzne preto v tejto kapitole zhodnotím reakcie a dopady v jednotlivých zapojeniach.

Ako prvé musím spomenúť samotné konfigurácie smerovačov. Na smerovačoch firmy Cisco stačí spustiť smerovací proces pre distribúciu multicastu (napríklad PIM) a smerovač začne prenášať dáta od zdroja na príjemcov. Pri zariadeniach Huawei je nutné v mieste, kde je pripojená užívateľská stanica (príjemca multicastu) aktivovať na rozhraní protokol IGMP, aby začalo zariadenie prijímať žiadosti o zaradenie do skupiny.

Pri testovaní IGMP snooping spolupracovali zariadenia bez problémov. Avšak na oko sa zdalo, že po spustení multicastového vysielania bol prepínač od firmy Cisco (pripojený k smerovaču Huawei) schopný rýchlejšie spracovať údaje (rýchlejšie sa začalo video zobrazovať na prijímacej stanici). Naproti tomu, v debugu tohto zariadenia sa počas prenosu objavilo pár chybových hlásení. Tieto chyby však nemali nejaký vážny dopad na distribúciu multicastu. Na prepínači od firmy Huawei išlo všetko bez známky problému.

Pri testovaní MLD Snooping sa na začiatku testovania zdalo, že funguje len medzi smerovačom Huawei a prepínačom Cisco. Varianta smerovač Cisco a prepínač Huawei neustále broadcastovala multicast na všetky porty. Neskôr, po dôkladnom prehliadnutí kontrolných výpisov som zistil, že na prepínači Huawei je MLD v základnom stave nastavený na verziu 1. Preto po prenastavení na verziu 2 začal fungovať správne aj MLD Snooping na prepínači Huawei.

Testovanie protokolu PIM-DM nebolo ničím zvláštne a fungovalo správne. Čo by stálo za zmienku je možnosť nastaviť protokol PIM u smerovača Cisco do sparse-dense modu čo mu tým pádom pridáva na modularite a človek čo zostavuje sieť nemusí premýšľať, čo bude prípadne na druhej strane nastavené. Cisco dokonca dovoľuje nastaviť jedno rozhranie ako PIM-DM a iné ako PIM-SM. U smerovačov spoločnosti Huawei toto nie je možné (prinajmenšom na zariadeniach, ktorými škola disponuje to možné nie je) akonáhle sa niektoré rozhranie nastaví do nejakého módu, povedzme PIM-DM, musia byť aj ostatné pripojené rozhranie v móde rovnakom.

Pri testovaní protokolu PIM-SM som skúšal rôzne možnosti určenia RP. Pri statickom RP fungovalo všetko bez problémov, konfigurácie sú veľmi podobné ale kladnejšie hodnotím spôsob nastavovania u Huawei. Celková orientácia je podľa môjho názoru logickejšia. Pre porozumenie uvediem príklad. Na to, aby som nastavil napríklad spomínané RP, musím najskôr vojsť do nastavení protokolu PIM a potom zadať príkaz na určenie

RP. U Cisca je to podobné ako s konfiguráciou statickej cesty a množstva iných príkazov, ktoré sa začínajú IP (pre určenie RP je to *ip pim rp-address*). Pri testovaní automatickej voľby RP som si všimol, že kým sa prvý prenos rozbehne trvá to citeľný čas. To ale nie je nič nečakané, pretože vzhľadom k počtu zariadení voľba RP a BSR niečo potrvá. Pre upresnenie, nie je to čas v merítku desiatok sekúnd, ale odhadom možno dve sekundy. V debugu síce neboli známky nezrovnalostí ale predpokladám, že to mohol zapríčiniť aj rozdielny prístup k určovaniu BSR a rozosielaniu RP kandidátov. Pri variante Anycast RP sa taktiež neprejavili žiadne väčšie problémy. Jediný prípad výpadku spojenia na dlhší čas bol v situácii, kedy som v krátkom časovom úseku viac krát zmenil vysielaciu stanicu a prijímače. Dialo sa v podstate to, že stanica bola v jednom okamihu zdrojom multicastu a krátko nato bola prijímačom a zdrojom sa stala zase iná stanica. Pri tomto počínaní zostala časť siete v podstate hluchá. Vo výpisoch síce prichádzali multicastové pakety k smerovaču, no on nebol schopný určiť na ktoré rozhranie ich predávať. Stalo sa to na smerovači Huawei a situácia sa javila vlastne ako keby zdroj posielal dáta sám sebe. V reálnej sieti je taká vysoká frekvencia zmien v podstate nemožná a chyba sa po vypršaní časovačov odstránila sama (prípadne, stačilo by vyčistiť multicastové informácie v pamäti smerovača).

Pri testovaní PIMv6 bolo možné otestovať len ekvivalent k PIM-SM, pretože podľa dokumentácie Cisco nemá ešte implementovanú Dense Mode verziu. Otestovanie čiste na platforme Huawei by nesplňovalo podmienku otestovania kompatibility medzi Ciscom a Huawei. A smerovač Huawei s podporou IPv6 multicastu je momentálne v škole k dispozícií len jeden, ako budem vysvetľovať neskôr.

Pri testovaní protokolu MBGP sa mi zdala konfigurácia zase niečo málo prívetivejšia práve na zariadení Huawei. Pretože v prípade, že treba zahrnúť nejakú priamo pripojenú sieť do smerovania je v BGP potrebné u Cisca zadať príkaz *network* a postupne pridať všetky takéto siete. U Huaweiu stačí jednoducho napísať *import route direct*. Pri testovaní tejto konfigurácie ma prekvapilo, že ako na smerovačoch Huawei, tak na smerovačoch Cisco neboli žiadne záznamy pri spustení debugu. Preto som bol pri hľadaní nezrovnalostí odkázaný len na odchytávanie prenosov pomocou Wiresharku na hube vloženom medzi smerovače.

U testovania MSDP sa v podstate pridalo prepojenie RP nad MBGP sieťou. V multicastovej časti konfigurácie bolo všetko v poriadku naproti tomu sa zase preukázala zložitosť konfigurácii smerovačov Cisco. Pri tomto zapojení boli v jednotlivých AS použité smerovacie protokoly OSPF, takže za účelom prepojenia týchto sietí bolo potrebné redis-

tribuovať smerovacie informácie do BGP a naopak. U smerovača Huawei stačí napísať vnútri smerovacieho procesu čo chceme doň zahrnúť napríklad v OSPF napíšeme *import-route BGP* u Cisca sú podobné nastavenia náročnejšie.

Posledným testovaným zapojením bol Multicast over GRE. Jedná sa v podstate o veľmi jednoduchú záležitosť vďaka ktorej by sme mohli v podstate prenášať multicastové dáta naprieč neznámu doménu. Táto topológia fungovala správne len v prípade, že bol zdroj multicastu za smerovačom Cisco. Pri pokuse o komunikáciu z opačnej strany, teda Od smerovača Huawei nastával problém s overením RPF. Tento problém som uzavrel ako nejakú internú záležistosť medzi týmito výrobcami, pretože nič z toho čo som nastavoval, by nemalo túto kolíziu spôsobovať. Doporučované riešenie na tento problém je aplikácia statickej cesty smerom k zdroju vysielania. Avšak poukazuje to na fakt, že Cisco v tomto prípade vyhodnocovalo informácie nesprávne a pokúšalo sa overovať spätnú cestu cez zlé rozhranie.

Za účelom testovania som bol nútený vykonať u Huaweiu update firmware ako už som spomínal v predchádzajúcich kapitolách. Pretože zariadenia, ktoré boli v škole prístupne nepodporovali IPv6 multicast. Tomu predchádzala zdĺhavá komunikácia s obchodným zástupcom spoločnosti Huawei, ktorý mi však firmware pre použitie v škole ochotne dodal. Návody na update som musel vyhľadávať na stránkach Huawei supportu. Pretože Google indexuje len malú časť informácii a dokumentácii, ktoré Huawei vydáva. Obyčajne vyhľadávanie prostredníctvom Google ponúka stránky zariadení H3C, ktoré údajne napriek tomu, že sa konfigurácie nápadne ponášajú na tie od Huawei nemajú spolu nič spoločné. Update som vykonal na jednom smerovači a jednom prepínači pretože na ostatné zariadenia by som musel získať ďalšie firmware.

Návody na konfigurácie a dokumentácie na väčšinu zariadení Cisco som vyhľadával pomocou Google (dostupné sú však na [25]) a pre zariadenia Cisco z materiálov na stránkach podpory [24]. Pri zariadeniach Cisco bol problém z IPv6 multicastom len na prepínači a ten sa dal ľahko vyriešiť nastavením duálneho režimu.

# 14 Záver

Cieľom tejto diplomovej práce bolo popísať problematiku multicastov a ich šírenia v sieti. Navrhnúť, realizovať a otestovať siete pre distribúciu multicastu v laboratórnom prostredí. V týchto sieťach som mal rovnako otestovať kompatibilitu zariadení Cisco a Huawei.

Aby som mohol otestovať, či navrhované siete skutočne fungujú, musel som nájsť spôsob ako generovať multicastové streamy. Prvým riešením bol VLC player, z ktorého som na jednej strane vysielal video a na druhej strane prijímal. Toto testovanie malo svoje nedostatky, nakoľko sa mi nepodarilo nájsť korektný spôsob ako nastaviť vysielanie pre IPv6. Preto som ako druhý spôsob generovania multicastu používal script v jazyku python. Tento script som používal hlavne pri protokoloch pracujúcich nad IPv6 prípadne pri väčších topológiach, kedy som bol nútený použiť na prepojenie smerovačov sériove linky.

Ako prvý som testoval IGMP Snooping. Táto konfigurácia fungovala medzi zariadeniami Cisco a Huawei bez problémov.

V nasledujúcej kapitole som testoval MLD Snooping, čo je vlastne ekvivalentom IGMP Snooping pre IPV6.

Pri testovaní protokolu PIM-DM išlo taktiež všetko bez problémov. Pri takto základnom protokole som zvolil veľmi jednoduchú topológiu o dvoch smerovačoch. Rozsiahlejšia topológia by nemala zmysel, pretože pri PIM-DM nie sú žiadne špeciálne úlohy, ktoré by smerovače mohli zastávať. Na otestovanie či tento protokol funguje a či funguje správne bola preto dostačujúca.

Protokol PIM-SM má rozsiahle možnosti použitia a aj konfigurácie. V úvode tejto kapitoly pracujem s rovnakou topológiou ako pri PIM-DM. Konkrétne ide o kapitolu pre statické nastavenie RP. Táto varianta funguje bez problémov. Ďalšou možnosťou je nastavenie pre automatickú voľbu RP. Toto nastavenie funguje správne. Poslednou variantou PIM-SM je konfigurácia známa ako Anycast RP. Je to zaujímave riešenie, ktoré využíva protokol MSDP. Ako hlavný prínos vnímam rozloženie záťaže a šikovné využitie unicastoveho smerovacieho protokolu na určenie najlepšej cesty. Pretože RP sú pod rovnakou IP adresou, o tom na ktorý z nich príde paket s multicastom rozhodne smerovacia tabuľka.

V kapitole PIMv6 som popisoval IPv6 variantu protokolu PIM-SM. Variantu PIM-DM som netestoval, pretože spoločnosť Cisco neposkytuje podporu pre túto konfiguráciu.

Konfigurácia MBGP, až na malú nejasnosť ohľadom klasifikovania pôvodu jednotlivých záznamov, fungovalo bez problémov. Jediné, čo by sa dalo vytknúť je zložitejšia konfigurácia, ale to pramení už z protokolu BGP. Konfigurácia MSDP fungovala správne. V tejto kapitole som sa už nevenoval rozpisu a vysvetleniu jednotlivých správ v debugu, pretože som to urobil pri Anycast RP. Tento protokol spolupracuje a funguje nad protokolom BGP, preto ho aj v rámci práce uvádzam vždy za ním.

Zaujímavým riešením prenosu multicastu je využitie tunelu. Prenos multicastu over GRE dokáže v podstate zabezpečiť transitovanie cez nejaký neznámi (cudzí) AS. Konfigurácia funguje správne, pokiaľ je zdroj vysielania umiestnený za smerovačom Cisco. Pokiaľ je zdroj za smerovačom Huawei, objaví sa u Cisca problém s overením RPF. Tento problém však poukazuje na to, že v tomto ohľade je smerovač Huawei bezproblémovejší.

Pri čítaní práce ste si mohli všimnúť, že topológie sú navrhnuté tak, aby ukázali všetky možnosti a boli čo možno najjednoduchšie na replikáciu. V prípade, že by čitateľ mal záujem moje testovania aplikovať sú v prílohách uvedené presné nastavenia jednotlivých smerovačov.

Pri praktickej časti tejto práce som sa zoznámil s konfiguráciami zariadení Huawei. Dovolím si tvrdiť, že aj keď na zariadeniach Cisco som zvyknutý pracovať, niektoré konfigurácie sa mi zdali na Huawei zrozumiteľnejšie. Pozdáva sa mi systém vnárania do jednotlivých nastavení a to, že sú niektoré príkazy kratšie. V čom sa však Ciscu nemôže Huawei vyrovnať sú dokumentácie. Huawei nemá indexované veľké množstvo materiálov, a dajú sa vyhľadať len priamo na stránkach Huawei supportu. Čo je ešte plusom pre Huawei je aktívne fórum na stránkach supportu, kde môže človek prispievať hneď po registrácii a nemusí byť ani overeným vlastníkom ich zariadenia. Naproti tomu, na Ciscu sa dá takmer všetko vyhľadať priamo prostredníctvom Google. A množstvo absolventov Cisco akadémii si vedie blogy, ktoré sú rovnako cennými zdrojmi informácií.

Jednotlivé konfigurácie môžu poslúžiť ako fregmenty pre poskladanie rozsiahlej topológie. Od prvej konfigurácie k poslednej by bolo možné zostaviť sieť začínajúcu na úrovni LAN a prechádzajúcu až do úrovne autonómnych systémov. Rovnako tieto konfigurácie dokazujú, že zaridenia Cisco a Huawei dokážu medzi sebou prenášať multicast na každej úrovni.

# 15 Literatúra

[1] P. Grygarek, *IP Multicast*, [online], 2005 [cit. 26.1.2015].
Dostupné z : <http://wh.cs.vsb.cz/sps/images/2/21/Multicast.pdf >

[2] IANA, *IPv4 Multicast Address Space Registrym*, [online], 17.12.2014 [cit. 26.1.2015].
Dostupné z : <http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml >

[3] S. Deering, *Host Extensions for IP Multicasting*, [online], August 1989 [cit. 26.1.2015].
Dostupné z : <https://tools.ietf.org/rfc/rfc1112.txt >

[4] W. Fenner, *Internet Group Management Protocol, Version 2*, [online], November 1997 [cit. 26.1.2015].
Dostupné z : <https://tools.ietf.org/html/rfc2236 >

[5] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan *Internet Group Management Protocol, Version 3*, [online], Oktober 2002 [cit. 26.1.2015].
Dostupné z : <https://tools.ietf.org/html/rfc3376 >

[6] T. Pusateri, *Distance Vector Multicast Routing Protocol*, [online], 22.10.2003 [cit. 26.1.2015].
Dostupné z : <https://tools.ietf.org/html/draft-ietf-idmr-dvmrp-v3-11 >

[7] K. Dooley,I.J. Brown, *Cisco Cookbook*, O'Reilly Media,Inc.,2003.

[8] INE, *Understanding BSR Protocol*, [online], 7.4.2009 [cit. 26.1.2015].
Dostupné z : <http://blog.ine.com/2009/04/07/understanding-bsr-protocol/ >

[9] Video LAN, *VLC Media Player*, [online], 26.7.2014 [cit. 26.1.2015].
Dostupné z : <http://www.videolan.org/vlc/ >

[10] Vimeo, *Short Films Download*, [online], 2004 [cit. 26.1.2015].
Dostupné z : <http://vimeo.com/album/2079687/ >

[11] Vimeo, *Fair Use*, [online], 2004 [cit. 26.1.2015].
Dostupné z : <http://vimeo.com/help/faq/legal-stuff/fair-use >

[12] Peak Drive, *How to use VLC Media player to stream multicast video*, [online], 12.12.2012 [cit. 26.1.2015]. Dostupné z : <http://peakdrive.com/?p=440 >

[13] Wireshark, *Download Wireshark*, [online], 2006 [cit. 26.1.2015].
Dostupné z : <https://www.wireshark.org/ >

[14] Python, *mcast.py*, [online],[cit. 26.1.2015].
Dostupné z : <http://svn.python.org/projects/python/trunk/Demo/sockets/mcast.py >

[15] Cisco, *Configuring IP Multicast Routing*, [online],[cit. 26.1.2015].
Dostupné z : <http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfmulti.html#wp1069177 >

[16] Ucl, *PIM-DM Example*, [online],23.7.203[cit. 26.1.2015].
Dostupné z : <http://www.hep.ucl.ac.uk/ ytl/multi-cast/pim-dm_01.html >

[17] Cisco, *Configuring a Rendezvous Point*, [online], 15.3.2002 [cit. 28.1.2015].
Dostupné z : <http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html >

[18] Laurent Prat, *Basic Multicast part 6 – Anycast RP*, [online], 1.12.2012 [cit. 28.1.2015].
Dostupné z : <https://aitaseller.wordpress.com/2012/12/01/basic-multicast-part-6-anycast-rp/ >

[19] Tomáš Podermański, Vladimír Veselý, *IPv6 Mýty a skutečnost, díl VII.*, [online], 24.3.2011 [cit. 26.4.2015].
Dostupné z : <http://www.lupa.cz/clanky/ipv6-myty-a-skutecnost-dil-vii-podpora-multicast-a-anycast-provozu/ >

[20] S. Deering, W. Fenner, B. Haberman, *Multicast Listener Discovery (MLD) for IPv6*, [online], 2.10.1999 [cit. 26.4.2015].
Dostupné z : <http://tools.ietf.org/html/rfc2710 >

[21] R. Vida, L. Costa, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*, [online], 12.6.2004 [cit. 26.4.2015].
Dostupné z : <http://tools.ietf.org/html/rfc3810 >

[22] P Bouška, *Jak multicast funguje* , [online], 10.3.2009 [cit. 26.4.2015].
Dostupné z : <http://www.samuraj-cz.com/clanek/tcpip-skupinove-vysilani-ip-multicast-a-cisco/ >

[23] B. Williamson, *Developing IP Multicast Networks, Volume I*, Cisco Press,2010.

[24] Huawei, *Product support*, [online], 2015 [cit. 28.4.2015].
Dostupné z : <http://support.huawei.com/enterprise/Main.action >

[25] Cisco, *Product support*, [online], 2015 [cit. 28.4.2015].
Dostupné z : <http://www.cisco.com/cisco/web/support/index.html >

[26] B. Fenner, D. Meyer, *Multicast Source Discovery Protocol (MSDP)*, [online], October 2015 [cit. 28.4.2015].
Dostupné z : <https://tools.ietf.org/html/rfc3618 >

# Prílohy

## Zoznam príloh

# A Zdrojový kód scriptu v jazyku Python

```
#!/usr/bin/env python
#
# Send/receive UDP multicast packets.
# Requires that your OS kernel supports IP multicast.
#
# Usage:
#    mcast -s (sender, IPv4)
#    mcast -s -6 (sender, IPv6)
#    mcast    (receivers, IPv4)
#    mcast -6 (receivers, IPv6)

MYPORT = 8123
MYGROUP_4 = '225.0.0.250'
MYGROUP_6 = 'ff15:7079:7468:6f6e:6465:6d6f:6d63:6173'
MYTTL = 1 # Increase to reach other networks

import time
import struct
import socket
import sys

def main():
    group = MYGROUP_6 if "-6" in sys.argv[1:] else MYGROUP_4

    if "-s" in sys.argv[1:]:
        sender(group)
    else:
        receiver(group)


def sender(group):
    addrinfo = socket.getaddrinfo(group, None)[0]

    s = socket.socket(addrinfo[0], socket.SOCK_DGRAM)

    # Set Time-to-live (optional)
    ttl_bin = struct.pack('@i', MYTTL)
    if addrinfo[0] == socket.AF_INET: # IPv4
        s.setsockopt(socket.IPPROTO_IP, socket.IP_MULTICAST_TTL, ttl_bin)
```

```
    else:
        s.setsockopt(socket.IPPROTO_IPV6, socket.IPV6_MULTICAST_HOPS, ttl_bin)

    while True:
        data = repr(time.time())
        s.sendto(data + '\0', (addrinfo[4][0], MYPORT))
        time.sleep(1)


def receiver(group):
    # Look up multicast group address in name server and find out IP version
    addrinfo = socket.getaddrinfo(group, None)[0]

    # Create a socket
    s = socket.socket(addrinfo[0], socket.SOCK_DGRAM)

    # Allow multiple copies of this program on one machine
    # (not strictly needed)
    s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)

    # Bind it to the port
    s.bind(('', MYPORT))

    group_bin = socket.inet_pton(addrinfo[0], addrinfo[4][0])
    # Join group
    if addrinfo[0] == socket.AF_INET: # IPv4
        mreq = group_bin + struct.pack('=I', socket.INADDR_ANY)
        s.setsockopt(socket.IPPROTO_IP, socket.IP_ADD_MEMBERSHIP, mreq)
    else:
        mreq = group_bin + struct.pack('@I', 0)
        s.setsockopt(socket.IPPROTO_IPV6, socket.IPV6_JOIN_GROUP, mreq)

    # Loop, printing any data we receive
    while True:
        data, sender = s.recvfrom(1500)
        while data[-1:] == '\0': data = data[:-1] # Strip trailing \0's
        print (str(sender) + '  ' + repr(data))


if __name__ == '__main__':
    main()
```

# B Konfigurácie smerovačov pre PIM DM

## B.1 Skrátená konfigurácia smerovača RAHuawei

```
 sysname RAHuawei
#

multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.2 255.255.255.252
 pim dm
#
interface GigabitEthernet0/0/1
 ip address 20.0.1.2 255.255.255.252
 pim dm
 igmp enable
#
interface GigabitEthernet0/0/2
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim dm
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 20.0.1.0 0.0.0.3
```

## B.2 Skrátená konfigurácia smerovača RBCisco

```
hostname RBCisco

!
no ip domain lookup
ip multicast-routing
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 ip pim dense-mode
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 ip pim dense-mode
 ip ospf 1 area 0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.252
 ip pim dense-mode
 ip ospf 1 area 0
 speed auto
 duplex auto
!
router ospf 1
```

# C Konfigurácie smerovačov pre PIM SM so statickým RP

## C.1 Skrátená konfigurácia smerovača RAHuawei

```
 sysname RAHuawei
#

multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 10.0.0.2 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 20.0.1.2 255.255.255.252
 pim sm
 igmp enable
#
interface GigabitEthernet0/0/2
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 20.0.1.0 0.0.0.3
#
PIM
 static-rp 3.3.3.3
#
```

## C.2 Skrátená konfigurácia smerovača RBcisco

```
hostname RBCisco

!
no ip domain lookup
ip multicast-routing
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 ip pim dense-mode
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 ip pim dense-mode
 ip ospf 1 area 0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.252
 ip pim dense-mode
 ip ospf 1 area 0
 speed auto
 duplex auto
!
router ospf 1
!
ip pim rp-address 3.3.3.3
```

# D Konfigurácie smerovačov pre PIM SM s automatickou voľbou RP

## D.1 Skrátená konfigurácia smerovača RAHuawei

```
sysname RAHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 20.0.1.2 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 20.0.2.1 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/2
 ip address 10.0.0.2 255.255.255.252
 pim sm
 igmp enable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 20.0.1.0 0.0.0.3
  network 20.0.2.0 0.0.0.3
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
```

## D.2 Skrátená konfigurácia smerovača RBHuawei

```
sysname RBHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 20.0.1.1 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 20.0.3.1 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/2
 ip address 20.0.4.1 255.255.255.252
 pim sm
 igmp enable
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 20.0.1.0 0.0.0.3
  network 20.0.3.0 0.0.0.3
   network 20.0.4.0 0.0.0.3
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
```

## D.3 Skrátená konfigurácia smerovača RCHuawei

```
sysname RCHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 20.0.2.2 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 20.0.3.2 255.255.255.252
 pim sm
#

interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 20.0.2.0 0.0.0.3
  network 20.0.3.0 0.0.0.3
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
```

## D.4 Skrátená konfigurácia smerovača RACisco

```
hostname RACisco
!
no ip domain lookup

!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Serial1/0
 ip address 10.0.4.1 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 clock rate 64000
!
interface Serial1/1
 ip address 10.0.3.1 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 clock rate 64000
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
```

## D.5 Skrátená konfigurácia smerovača RBCisco

```
hostname RBCisco
!
no ip domain lookup

!
interface Loopback0
 ip address 6.6.6.6 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Serial1/0
 ip address 10.0.3.2 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Serial1/1
 ip address 10.0.2.2 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
```

## D.6 Skrátená konfigurácia smerovača RCCisco

```
hostname RCCisco
!
no ip domain lookup

!
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.0.1.1 255.255.255.252
 ip pim dense-mode
 ip ospf 1 area 0
!
interface Serial1/0
 ip address 10.0.4.2 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Serial1/1
 ip address 10.0.2.1 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 clock rate 64000
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
```

# E Konfigurácie prepínačov pre IGMP Snooping

## E.1 Skrátená konfigurácia prepínača Huawei

```
sysname HUswitch
#
multicast routing-enable
#
igmp-snooping enable
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/22
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/23
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/24
 port link-type access
 port default vlan 100
#
```

## E.2 Skrátená konfigurácia prepínača Cisco

```
hostname Switch
!
ip igmp snooping
!
vlan 100
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport mode access
```

# F Konfigurácie prepínačov pre MLD Snooping

## F.1 Skrátená konfigurácia smerovača Huawei

```
#
sysname Quidway
#
multicast ipv6 routing-enable
#
mld-snooping enable
#
vlan 100
 mld-snooping enable
 mld-snooping version 2
#
interface MEth0/0/1
 ip address 192.168.50.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/22
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/23
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/24
 port link-type access
 port default vlan 100
#
```

## F.2 Skrátená konfigurácia prepínača Cisco

```
hostname Switch
!
vlan 100
!
ipv6 mld snooping
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport mode access
!
```

# G Konfigurácie smerovačov pre PIM SM Anycast RP

## G.1 Skrátená konfigurácia smerovača RAHuawei

```
sysname RAHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 1.2.3.18 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 1.2.3.13 255.255.255.252
 pim sm
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface LoopBack10
 ip address 10.10.10.10 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
  network 1.2.3.12 0.0.0.3
  network 1.2.3.16 0.0.0.3
  network 2.2.2.2 0.0.0.0
  network 10.10.10.10 0.0.0.0
#
pim
 static-rp 10.10.10.10
#
msdp
 originating-rp LoopBack0
 peer 1.1.1.1 connect-interface LoopBack0
#
```

## G.2 Skrátená konfigurácia smerovača RBHuawei

```
sysname RBHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 1.2.3.10 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 1.2.3.14 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/2
 ip address 10.0.0.1 255.255.255.252
 pim sm
 igmp enable
#
ospf 1
 area 0.0.0.0
  network 1.2.3.8 0.0.0.3
  network 1.2.3.12 0.0.0.3
  network 10.0.0.0 0.0.0.3
#
pim
 static-rp 10.10.10.10
#
```

## G.3 Skrátená konfigurácia smerovača RCHuawei

```
 sysname RCHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 1.2.3.9 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 1.2.3.6 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/2
 ip address 30.0.0.1 255.255.255.252
 pim sm
 igmp enable
#
ospf 1
 area 0.0.0.0
  network 1.2.3.4 0.0.0.3
  network 1.2.3.8 0.0.0.3
  network 30.0.0.0 0.0.0.3
#
pim
 static-rp 10.10.10.10
#
```

## G.4 Skrátená konfigurácia smerovača RACisco

```
hostname RACisco
!
no ip domain lookup
!
ip multicast-routing
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Loopback10
 ip address 10.10.10.10 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface FastEthernet0/1
 ip address 1.2.3.5 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 1.2.3.2 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
!
router ospf 1
 log-adjacency-changes
!
ip pim rp-address 10.10.10.10
ip msdp peer 2.2.2.2 connect-source
      Loopback0
ip msdp originator-id Loopback0
!
```

## G.5 Skrátená konfigurácia smerovača RBCisco

```
hostname RBCisco
!
no ip domain lookup
!
ip multicast-routing
!
interface FastEthernet0/0
 ip address 20.0.0.1 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 1.2.3.21 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 no fair-queue
 clock rate 128000
!
interface Serial0/1/1
 ip address 1.2.3.1 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 clock rate 128000
!
router ospf 1
 log-adjacency-changes

        !
ip pim rp-address 10.10.10.10
!
```

## G.6 Skrátená konfigurácia smerovača RCCisco

```
hostname RCCisco
!
no ip domain lookup
!
ip multicast-routing
!
interface FastEthernet0/0
 ip address 1.2.3.17 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 1.2.3.22 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 no fair-queue
!
router ospf 1
 log-adjacency-changes
!
ip pim rp-address 10.10.10.10
!
```

# H Konfigurácie smerovačov PIMv6

## H.1 Skrátená konfigurácia smerovača RAHuawei

```
sysname RAHuawei
#
ipv6
#
router id 1.1.1.1
#
multicast ipv6 routing-enable
#
ospfv3 1
 router-id 1.1.1.1
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 2001:1::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address 2001:10::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
 mld enable
#
pim-ipv6
 static-rp 2001:1::1
#
```

## H.2 Skrátená konfigurácia smerovača RBCisco

```
hostname RBCisco
!
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:1::2/64
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:20::1/64
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
!
ipv6 pim rp-address 2001:1::1
!
```

# I Konfigurácie sperovačov MBGP

## I.1 Skrátená konfigurácia smerovača RAHuawei

```
sysname RAHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 2.2.2.1 255.255.255.0
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet0/0/2
 ip address 1.1.1.1 255.255.255.0
 pim sm
#
bgp 100
 peer 1.1.1.2 as-number 100
 peer 2.2.2.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 1.1.1.2 enable
  peer 2.2.2.2 enable
 #
 ipv4-family multicast
  undo synchronization
  import-route direct
  peer 1.1.1.2 enable
  peer 2.2.2.2 enable
#
pim
 static-rp 2.2.2.2
#
```

## I.2 Skrátená konfigurácia smerovača RBHuawei

```
sysname RBHUawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 30.0.0.1 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet0/0/1
 ip address 3.3.3.2 255.255.255.0
 pim sm
#
bgp 300
 peer 3.3.3.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 3.3.3.1 enable
 #
 ipv4-family multicast
  undo synchronization
  import-route direct
  peer 3.3.3.1 enable
#
pim
 static-rp 2.2.2.2
```

## I.3 Skrátená konfigurácia smerovača RACisco

```
hostname RACisco
!
!
no ip domain lookup
ip multicast-routing
!
interface Loopback0
 ip address 100.100.100.100
       255.255.255.255
!
interface FastEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 3.3.3.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 3.3.3.2 remote-as 300
 !
 address-family ipv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 next-hop-self
 neighbor 3.3.3.2 activate
 no auto-summary
 no synchronization
 network 100.100.100.100 mask
       255.255.255.255
 exit-address-family
 !
 address-family ipv4 multicast
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 next-hop-self
 neighbor 3.3.3.2 activate
 no auto-summary
 no synchronization
 exit-address-family
!
ip pim rp-address 2.2.2.2
!
```

## I.4 RBCisco

```
hostname RBCisco
!
no ip domain lookup
ip multicast-routing
!
interface FastEthernet0/0
 ip address 2.2.2.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 20.0.0.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 2.2.2.1 remote-as 100
 !
 address-family ipv4
 neighbor 2.2.2.1 activate
 no auto-summary
 no synchronization
 network 20.0.0.0 mask 255.255.255.0
 exit-address-family
 !
 address-family ipv4 multicast
 neighbor 2.2.2.1 activate
 no auto-summary
 no synchronization
 network 20.0.0.0 mask 255.255.255.0
 exit-address-family
!
ip pim rp-address 2.2.2.2
!
```

# J Konfigurácie smerovačov pre MSDP

## J.1 Skrátená konfigurácia smerovača RAHuawei

```
 sysname RAHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 10.10.10.1 255.255.255.0
 pim sm
 igmp enable
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.2 255.255.255.252
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 10.10.10.0 0.0.0.255
#
```

## J.2 Skrátená konfigurácia smerovača RBHuawei

```
sysname RBHuawei
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 1.0.0.1 255.255.255.252
 pim sm
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.252
 pim sm
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
bgp 100
 router-id 1.1.1.1
 peer 1.0.0.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  import-route ospf 1
  peer 1.0.0.2 enable
 #
 ipv4-family multicast
  undo synchronization
  peer 1.0.0.2 enable
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.0.0.0 0.0.0.3
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 1.0.0.2 connect-interface
      GigabitEthernet0/0/0
#
```

## J.3 Skrátená konfigurácia smerovača RACisco

```
hostname RACisco
!
no ip domain lookup
ip multicast-routing
!
interface FastEthernet0/0
 ip address 20.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 20.0.0.2 255.255.255.252
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
!
```

## J.4 Skrátená konfigurácia smerovača RBCisco

```
hostname RBCisco
!
ip cef
no ip domain lookup
ip multicast-routing
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
interface FastEthernet0/0
 ip address 1.0.0.2 255.255.255.252
 ip pim sparse-mode
!
interface FastEthernet0/1
 ip address 20.0.0.1 255.255.255.252
 ip pim sparse-mode
!
router ospf 1
 log-adjacency-changes
  redistribute bgp 200 subnets
 network 2.2.2.2 0.0.0.0 area 0
 network 20.0.0.0 0.0.0.3 area 0
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 1.0.0.1 remote-as 100
 !
 address-family ipv4
   redistribute ospf 1 match internal
        external 1 external 2
  neighbor 1.0.0.1 activate
  no auto-summary
  no synchronization
  network 20.0.0.0 mask 255.255.255.252
 exit-address-family
 !
 address-family ipv4 multicast
  neighbor 1.0.0.1 activate
  no auto-summary
 exit-address-family
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
ip msdp peer 1.0.0.1 connect-source
      FastEthernet0/0
!
```

# K Konfigurácie smerovačov pre Multicast over GRE

## K.1 Skrátená konfigurácia smerovača RAhuawei

```
 sysname RAHuawei
#
router id 2.2.2.2
#
multicast routing-enable
#
interface GigabitEthernet0/0/0
 ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
 pim sm
 igmp enable
#
interface LoopBack0
 ip address 10.10.1.1 255.255.255.255
#
interface Tunnel0/0/1
 mtu 1400
 tcp adjust-mss 1360
 ip address 192.168.10.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 10
 source LoopBack0
 destination 10.10.1.2
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.10.1.1 0.0.0.0
  network 192.168.100.0 0.0.0.255
#
pim
 c-bsr Tunnel0/0/1
 c-rp Tunnel0/0/1
```

## K.2 Skrátená konfigurácia smerovača RBCisco

```
hostname RBCisco
!
no ip domain lookup
ip multicast-routing
!
interface Loopback0
 ip address 10.10.1.2 255.255.255.255
 ip ospf 1 area 0
!
interface Tunnel0
 ip address 192.168.10.2 255.255.255.0
 ip mtu 1400
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 keepalive 10 3
 tunnel source Loopback0
 tunnel destination 10.10.1.1
!
interface FastEthernet0/0
 ip address 192.168.100.2 255.255.255.0
 ip ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.2.1.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
!
router ospf 1
 router-id 1.1.1.1
!
ip pim bsr-candidate Tunnel0 0
ip pim rp-candidate Tunnel0
```